DePaul University
University Libraries

DePaul Law Review

Volume 66
Issue 2 *Winter 2017: Twenty-Second Annual Clifford Symposium on Tort Law and Social Policy*

Article 3

Can Data Breach Claims Survive the Economic Loss Rule?

Catherine M. Sharkey

CAN DATA BREACH CLAIMS SURVIVE THE ECONOMIC LOSS RULE?

*Catherine M. Sharkey**

I. INTRODUCTION

In our highly interconnected, Internet-driven age, data security breaches pose a formidable regulatory challenge.[1] An age-old debate regarding the appropriate mix of standards (ex ante regulation versus ex post litigation), enforcement mechanisms (public agencies versus decentralized private enforcement), and federalism components (national versus state-by-state regulatory efforts) is playing out in real time with a cacophonous mix of emerging federal and state legisla-

* Crystal Eastman Professor of Law, New York University School of Law. Caleb Seeley (NYU Law 2017) and Peter Steffensen (NYU Law 2017) provided excellent research assistance. I presented earlier versions of this Article at the *22nd Annual Clifford Symposium on Tort Law and Social Policy*, the NYU Summer Faculty Workshop, the 2016 Privacy + Security Forum, and the Seton Hall Law Faculty Workshop, where I received helpful comments and suggestions from participants, especially Danielle Citron, Mark Geistfeld, Zachary Goldman, David Hoffman, Stephan Landsman, Alex Lipton, Florencia Marotta-Wurgler, David Opderbeck, Robert Rabin, Shauhin Talesh, and Katrina Wyman. The Filomen D'Agostino and Max E. Greenberg Research Fund provided generous summer research support.

1. Data security breaches impose significant costs. Recent studies report average firm costs per data breach incident in the range of one to eight million dollars. *See, e.g.*, Roberta D. Anderson, *Viruses, Trojans and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz*, 49 TORT TRIAL & INS. PRAC. L.J. 529, 542 (2014) ("The Ponemon Institute's *2012 Cyber Crime Study* found that 'the average annualized cost of cyber crime for 56 organizations in [its] study is $8.9 million per year, with a range of $1.4 million to $46 million.' This number is up from the $8.4 million average annualized cost reflected in the 2011 survey." (alteration in original) (footnotes omitted) (quoting PONEMON INST., 2012 COST OF CYBER CRIME STUDY: UNITED STATES 1 (2012), https://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf)); *id*. at 541 ("The 2011 high-profile attack on the Sony PlayStation Network alone was estimated to cost some $170 million."); Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 QUINNIPIAC L. REV. 369, 372 (2015) ("The average cost of a malicious data breach in the United States [from 2012 to 2013 was] . . . $7,155,402."); *see also* Pa. State Emps. Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 322 (M.D. Pa. 2005) ("'[T]o mitigate the damage caused by the compromise of PSECU members' Visa card magnetic stripe information, PSECU canceled' the 20,029 Visa cards . . . 'to protect its legal rights and to fulfill a contractual obligation owed to its customers.' The cancellation and reissuance cost PSECU $98,128.13." (citations omitted) (quoting Amended Complaint ¶¶ 39, 65, *Pa. State Emps. Credit Union*, 398 F. Supp. 2d at 317 (No. CV-04-1554), 2005 WL 4341834)).

tion,[2] agency enforcement actions,[3] state law enforcement,[4] and private class action litigation.

---

2. *E.g.*, 15 U.S.C. § 6801 (2012) (imposing an affirmative obligation on financial institutions to protect the security and confidentiality of customers' nonpublic personal information); 42 U.S.C. § 1320d (2012) (setting requirements and standards for health care providers' management of individually identifiable health information); 45 C.F.R. § 160.103 (2016) (implementing 42 U.S.C. § 1320d); 45 C.F.R. §§ 164.400–164.414 (2016) (providing for notification in the event of a breach of protected health information).

Forty-seven of the fifty states have notification statutes that require prompt notice of data breaches to those affected and to the attorney general. *See, e.g.*, FLA. STAT. § 501.171 (2016) (requiring notice for security breaches of personal information); MASS. GEN. LAWS ch. 93H, § 3 (Supp. 2016); MINN. STAT. § 325E.61 (2016); N.Y. GEN. BUS. LAW § 899-aa (McKinney Supp. 2016). Three states—Minnesota, Nevada, and Washington—take statutory protection a step further. *See, e.g.*, MINN. STAT. § 325E.64 (2016) (prohibiting the retention of personal credit or debit card information and imposing liability on the breaching party to the card issuer in the event of violation and damages); NEV. REV. STAT. § 603A.215 (2015) (requiring any data collector doing business in the state to comply with the current version of the Payment Card Industry Data Security Standards (PCI-DSS)); WASH. REV. CODE § 19.255.020 (2016) (governing the liability of credit card vendors and processors in the event of a breach). These statutory provisions are discussed further *infra* notes 216–17 and accompanying text.

3. *E.g.*, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd*, 799 F.3d 236, 259 (3d Cir. 2015); *see* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 636–37 (2014); Press Release, Fed. Trade Comm'n, Cord Blood Bank Settles FTC Charges that It Failed to Protect Consumers Sensitive Personal Information (Jan. 28, 2013), https://www.ftc.gov/news-events/press-releases/2013/01/cord-blood-bank-settles-ftc-charges-it-failed-protect-consumers; Press Release, Fed. Trade Comm'n, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009), https://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial; Press Release, Fed. Trade Comm'n, Dave & Buster's Settles FTC Charges It Failed to Protect Consumers' Information (Mar. 25, 2010), https://www.ftc.gov/news-events/press-releases/2010/03/dave-busters-settles-ftc-charges-it-failed-protect-consumers; Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against Cbr Systems, Inc. (May 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-approves-final-order-settling-charges-against-cbr-systems-inc; Press Release, Fed. Trade Comm'n, FTC Charges that Security Flaws in RockYou Game Site Exposed 32 Million Email Addresses and Passwords (Mar. 27, 2012), https://www.ftc.gov/news-events/press-releases/2012/03/ftc-charges-security-flaws-rockyou-game-site-exposed-32-million; Press Release, Fed. Trade Comm'n, FTC Settles Charges Against Two Companies that Allegedly Failed to Protect Sensitive Employee Data (May 3, 2011), https://www.ftc.gov/news-events/press-releases/2011/05/ftc-settles-charges-against-two-companies-allegedly-failed; Press Release, Fed. Trade Comm'n, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

4. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 752–54 (2016). Sometimes the state legislature makes express data breach enforcement choices. California, for example, creates a private right of action. *See* CAL. CIV. CODE §§ 1798.29, 1798.93 (2014) (requiring disclosure of security breaches by agencies that maintain data and establishing and creating a private action to recover actual damages resulting from identity theft). Illinois, by contrast, gives enforcement power exclusively to the attorney general under state consumer protection law. *See* 815 ILL. COMP. STAT. 530/40 (Supp. 2016).

This Article focuses on the emerging credit card data breach class action litigation and one formidable obstacle such litigation has encountered: the economic loss rule.[5] In its broadest terms, the economic loss rule posits that, absent physical injury or damage to property, there can be no tort recovery for negligent conduct that causes purely financial losses.[6] Merchants and intermediary credit card processors have raised the economic loss rule as a bar to recovery against claims for negligence and negligent misrepresentation brought by two classes of plaintiffs: (1) individual consumers whose credit card information has been stolen, and (2) banks and other financial institu-

5. Another frequent roadblock—not considered here—is lack of an injury in fact. Federal courts have repeatedly determined that plaintiffs lack Article III standing to bring suit. The future potential injury that may result from someone obtaining personal information when no fraudulent charges have been made has been deemed too speculative to qualify as an injury in fact. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) ("[A]llegations of hypothetical, future injury are insufficient to establish standing [in a data breach case]."); Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) ("[T]he potential threat of identity theft or identity fraud, to the extent any exists in this case, does not confer standing."); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 653–60 (S.D. Ohio 2014) (finding no injury-in-fact in data breach suit for increased risk of harm, loss of privacy, and loss of value of plaintiff's personally identifiable information); *In re* Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013) ("Merely alleging an increased risk of identity theft or fraud is insufficient to establish standing."). *But see* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (finding future injuries such as increased risk of fraudulent charges and identity theft due to stolen data are "concrete enough to support a lawsuit"); Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 696–97 (7th Cir. 2015) (finding that the alleged future risk was substantial enough to satisfy the injury-in-fact requirement of standing); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding that "a credible threat of real and immediate harm stemming from the theft of a laptop containing [plaintiffs'] unencrypted personal data" was sufficient to establish injury-in-fact).

In the face of restrictive rulings on standing, plaintiffs have sought recovery for credit monitoring—a present, realized cost—drawing an explicit parallel to medical monitoring actions. *See, e.g.*, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 970 (S.D. Cal. 2014) (noting that, as with medical monitoring, recovery of credit monitoring costs in data breach cases "requires a plaintiff to plead both a logical and temporal connection between the decision to purchase credit monitoring services and the defendant's alleged breach," which is a "high burden"); Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 914 (N.D. Cal. 2009) (expressing doubt that data breach cases and medical monitoring cases are analogous).

6. *Economic-Loss Rule*, BLACK'S LAW DICTIONARY (10th ed. 2014); *see* Dan B. Dobbs, *An Introduction to Non-Statutory Economic Loss Claims*, 48 ARIZ. L. REV. 713, 713 (2006) ("The stand-alone or 'pure' economic loss covered by the economic loss rule refers to pecuniary or commercial loss that does not arise from actionable physical, emotion or reputational injury to persons or physical injury to property."); *see also* Peter Benson, *The Problem with Pure Economic Loss*, 60 S.C. L. REV. 823, 823 (2009) ("For well over a century, it has been a settled feature of American and English tort law that in a variety of situations there is no recovery in negligence for pure economic loss, that is, for economic loss unrelated to injury to the person or the property of the plaintiff.").

tions who have suffered financial losses due to reimbursements for fraudulent charges or reissuing cards.[7]

Scholars have argued that the economic loss rule—a "venerable chestnut of tort law"[8]—sharply limits or altogether precludes potential tort liability for cybersecurity lapses. In turn, the rule hampers tort law's salience as a way to force actors to internalize the costs of the external harms they cause.[9] What is thus far missing from the debate, however, is a more fine-tuned account of the workings of the economic loss rule in this doctrinal context. This Article tackles this challenge and a more varied picture emerges. Namely, the extent to which the economic loss rule serves as a formidable barrier to credit card data security breach cases depends upon the underlying state law; in particular, whether a state adopts the majority or minority position on the rule, as well as how it defines various exceptions thereto. The doctrinal landscape unearthed here is consistent with recent empirical findings in data breach litigation that report a settlement rate that is appreciably higher than what is implied in the legal literature to date touting essentially no liability risk.[10]

---

7. *See, e.g.*, Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 423 (5th Cir. 2013); *In re* Home Depot, Inc. Customer Data Sec. Breach Litig., No. 14-md-2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016). In addition to claims of negligence and negligent misrepresentation, plaintiffs often allege statutory violations of consumer protection statutes and data breach notification statutes; negligence per se based on the violation of state or federal unfair or deceptive trade acts; breach of implied contract and/or contract; as well as unjust enrichment. *See generally* Catherine Palo, *Liability of Businesses to Governments and Consumers for Breach of Data Security for Consumers' Information*, 152 AM. JUR. 3D *Proof of Facts* 209 (2016).

8. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1535 (2013).

9. *See* Keith N. Hylton, *Property Rules, Liability Rules, and Immunity: An Application to Cyberspace*, 87 B.U. L. REV. 1, 14 (2007) (arguing that where transaction costs are high—as Hylton argues they are apt to be in cyberspace—a negligence (liability) rule is the best way to control externalities); Vincent R. Johnson, *Cybersecurity, Identify Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 275 (2005) (imposing negligence liability "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"); *see also* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 283–86 (2007) (arguing for a strict liability approach to data breaches, relying on a Calabresian cheapest cost avoider rationale, among others).

10. *See* Sasha Romanosky et al., *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 102 (2014). The authors report an overall settlement rate of known federal data breach lawsuits of 52% (86/164), which is "much higher than legal privacy scholarship would suggest." *Id.* at 93. Prior scholarship had suggested effectively no liability risk at all, and would thus predict no settlement. By contrast, the authors demonstrate that there is a real (albeit relatively small) risk of liability and that filed cases settle at the theoretically normal rate. More specifically, they report a 3.7% filing rate for data breaches, which could be interpreted as a lower bound, given that they exclude state courts and, with respect to federal courts, they rely exclusively on hand collected cases. The authors likewise point out that their empirical findings "could also be useful to insurance markets as a means of assessing a firm's risk." *Id.* at 102.

This Article's findings have significant implications for the emerging cybersecurity insurance field, especially in terms of assessing firms' overall liability exposure, and suggest that firms (at least those facing tort liability in certain jurisdictions that either do not employ the economic loss rule, or have weak versions in place) should pay more attention to the third-party liability portions of such policies.[11] Moreover, this Article raises the question whether, as a more robust third-party liability insurance market emerges in response to a greater threat of tort liability, insurers will engage in further risk management, exerting more potent regulatory control.[12]

The authors do not make any comments on the geographical distribution of their data, which consists exclusively of federal data breach lawsuits. It would be interesting to investigate whether the different state legal regimes have any impact on the number or types of breaches in particular states; and whether there are any behavioral response implications, in terms of either firms' taking additional data security precautions or adapting their corporate activity in any fashion.

11. Cyberinsurance policies typically cover both first- and third-party losses arising from a cyber incident. *See* Podolak, *supra* note 1, at 374–75. But, to date, the first-party component has attracted more attention. *See* NAT'L PROTECTION & PROGRAMS DIRECTORATE, U.S. DEP'T OF HOMELAND SEC., CYBERSECURITY INSURANCE WORKSHOP READOUT REPORT 1 (2012) [hereinafter 2012 WORKING GROUP], https://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf ("Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, network damage, and cyber extortion."); *see also* Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Liability Insurance: How Insurance Companies Act as "Compliance Managers" for Business*, 42 LAW & SOC. INQUIRY (forthcoming 2017) (manuscript at 14 n.52) (on file with *DePaul Law Review*) ("Whereas most companies did not have cyber insurance a decade ago, one in three organizations now have insurance specifically protecting against cyber and data theft losses."). Talesh's evidence suggests that, at present, firms are very interested in the first-party liability components of cybersecurity insurance policies. *See id*. at 16–17 (presenting evidence—based on interviews, participant observation at cyber liability insurance conferences, and analysis of insurer loss prevention manuals and risk management services—that firms seek various services offered by insurance companies, namely forensic experts, public relations firms, credit monitoring/restoration and legal services, primarily to deal with regulatory compliance issues).

"Third-party policies, by contrast, cover losses that a company causes to its customers and others, such as harms arising from the exposure of personally identifiable information (PII) through a data breach." NAT'L PROTECTION & PROGRAMS DIRECTORATE, U.S. DEP'T OF HOMELAND SEC., INSURANCE INDUSTRY WORKING SESSION READOUT REPORT: INSURANCE FOR CYBER-RELATED CRITICAL INFRASTRUCTURE LOSS: KEY ISSUES 1 n.1 (2014) [hereinafter 2014 WORKING GROUP], https://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf. There is evidence, moreover, that the market for third-party liability insurance is growing. *See* 2012 WORKING GROUP, *supra*, at 1, 9 (noting that the market for first-party cyberinsurance policies, which are "expensive, rare, and largely unattractive," is lagging behind the third-party market).

12. *See, e.g.*, Catherine M. Sharkey, *Revisiting the Noninsurable Costs of Accidents*, 64 MD. L. REV. 409, 437–38 (2005) (describing the risk management function of insurance). The role of insurance as risk management various significantly by insurance line, market conditions and the like. *See, e.g.*, RICHARD V. ERICSON ET AL., INSURANCE AS GOVERNANCE 267–310 (2003); Tom Baker & Rick Swedloff, *Regulation by Liability Insurance: From Auto to Lawyers Professional Liability*, 60 UCLA L. REV. 1412, 1416–23 (2013) (developing a conceptual framework for insurance as governance across different liability areas based upon risk-based pricing, underwriting,

Data security breach cases are fertile ground to explore the impact of the economic loss rule and to challenge the conceptual underpinnings of this judge-made doctrine. At present, there is a great deal of confusion on the part of courts as to whether and how the economic loss rule should apply. The second main goal of this Article is to provide both a conceptual framework for courts' resolution of data breach cases and a sound normative justification. Upon closer examination, it becomes clear that the rule operates in a fundamentally distinct manner in the "stranger paradigm" as compared to the "contracting parties paradigm." In the stranger paradigm—when an actor's negligence causes financial losses to a party with whom the actor has no pre-existing relationship—courts have deployed the economic loss rule to stave off the ripple effect or floodgates of unlimited liability.[13] Courts' overriding concern is that, should they impose tort liability for purely financial losses—which unlike physical harms tend to cascade forward in an unforeseeable (and uncontrollable) manner, impacting business and financial relationships down an endless chain—defendants will face potentially unlimited and disproportionate liability for their negligent actions.[14] Thus, the economic loss rule draws the line for *negligence* liability (i.e., the parameters of the duty of reasonable care) at physical injuries and property damage.[15]

In fairly sharp contrast, the overriding question for courts confronting the "contracting parties paradigm" is not whether a duty is owed, but what is the nature of that duty. Specifically, the question is whether a duty should be imposed *by law*, regardless of, or over and above, any voluntary allocation of risks and responsibilities already

---

contract design, claims management, loss prevention services, research and education, and engagement with public regulators).

The Department of Homeland Security's (DHS) National Protection and Programs Directorate assists private and public sector partners' efforts to secure cyber networks. In recent years, DHS has held workshops to examine "the ability of insurance carriers to offer relevant coverage at reasonable prices in return for the adoption of cyber risk management . . . procedures." 2014 WORKING GROUP, *supra* note 11, at 1. Nonetheless, these efforts are hampered by the fact that "no commonly agreed-to cybersecurity risk management standards, best practices, or metrics exist—a state of affairs that hinders the ability of carriers to conduct risk comparisons across companies." 2012 WORKING GROUP, *supra* note 11, at 4; *see also* 2014 WORKING GROUP, *supra* note 11, at 4 (noting that cyber risk actual tables, which are essential for providing insurance, are largely undeveloped).

13. Courts have articulated this concern alternately in terms of no proximate cause and no duty rulings as a matter of law.

14. *See, e.g.*, Dobbs, *supra* note 6, at 715 ("Stand-alone economic loss often spreads without limit.").

15. Note that this barrier does not pertain to intentional torts, such as fraud and intentional interference with contract. Here, presumably the intent prong serves to delimit liability, and there is no corresponding fear of over-deterrence.

made between the contracting parties. In other words, it is here that the economic loss rule functions primarily as a form of "border control," policing the boundaries of tort and contract.[16]

What makes the credit card data security breach cases so vexing is that they often straddle the stranger/contracting parties paradigms. They comprise a distinct form of "third party cases"—where the victims and defendants are not themselves in a contractual relationship, but nonetheless, they typically contract with a common entity, and thus are tied together through a complex web of contracts.[17] One federal district court described this web as follows:

> Issuer banks . . . issue credit cards to consumers. Acquirer banks . . . process payments for the merchants who make credit-card sales. When a consumer makes a credit-card purchase, the merchant swipes the card, sending a message to the acquirer bank. The acquirer bank then contacts the issuer bank to determine whether sufficient credit exists in the account. If so, the issuer bank clears the transaction, relays the message to the acquirer bank, which notifies the merchant. On a daily basis, the issuer bank forwards payment to the acquirer bank, which deposits the payment into the merchant's account.[18]

Typically, plaintiff issuer banks and defendant merchants and acquiring banks are members of the credit card networks (e.g., Visa and MasterCard), and thus are subject to the networks' regulations and

---

16. *See* William Powers, Jr., *Border Wars*, 72 TEX. L. REV. 1209, 1229 (1994) ("[I]n border wars between contract law and tort law, contract law itself should tell us which body of law should control. If contract law purports to decide the case, the negligence paradigm . . . should stay in the background."); *see also* Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 WASH. & LEE L. REV. 523, 546 (2009) ("If there is a convincing rationale for the economic loss rule, it is that the rule performs a critical boundary-line function, separating the law of torts from the law of contracts.").

17. Third-party cases are common in the sphere of negligent misrepresentation, the canonical example being that of a negligent accountant who furnishes an erroneous audit to a client, which is then relied upon by some third-party making a loan to that entity. *See* Ultramares Corp. v. Touche, 174 N.E. 441, 443–48 (N.Y. 1931); RESTATEMENT (SECOND) OF TORTS § 552 (AM. LAW INST. 1976). The third-party prototypical negligence action involves so-called three-cornered construction disputes, whereby a construction project manager contracts separately with an architect and construction company (who have no contract between them) and the negligence of the architect causes significant delay and increased costs to the construction company, who then sues the architect for negligence. *See* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR ECONOMIC HARM § 6 cmt. b (AM. LAW INST. 2014); *see, e.g.*, United States v. Spearin, 248 U.S. 132, 133–37 (1918); L.A. Unified Sch. Dist. v. Great Am. Ins. Co., 234 P.3d 490, 492–94 (Cal. 2010); BRW, Inc. v. Dufficy & Sons, Inc., 99 P.3d 66, 67–68 (Colo. 2004); Ass'n of Apartment Owners of Newtown Meadows *ex rel.* Bd. of Dirs. v. Venture 15, Inc., 167 P.3d 225, 232–37 (Haw. 2007); Indianapolis-Marion Cty. Pub. Library v. Charlier Clark & Linard, P.C., 929 N.E.2d 722, 725 (Ind. 2010); Sensenbrenner v. Rust, Orling & Neale, Architects, Inc., 374 S.E.2d 55, 56 (Va. 1988).

18. *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., No. H-10-171, 2011 WL 1232352, at *2 (S.D. Tex. Mar. 31, 2011).

contractual remedies.[19] Privity thus exists between the issuer bank and the payment card network, as well as between the acquirer bank and the payment card network. Privity does not exist between the issuer bank and the acquirer bank or credit card processor; nor does it always exist between consumer credit card holders and merchants.

Such third-party cases could be slotted into the stranger paradigm—on the theory that the victims (issuer banks or consumers) and defendants (merchants, acquirer banks, or credit card processing entities) are not in direct contractual privity. Alternatively, the cases could be treated as part and parcel of the consensual contracting parties paradigm on account of the web of contracts that link together victims and defendants. Courts have done both, though unpredictably. This Article aims to explore which makes more sense from a regulatory standpoint.

Part I explores the stranger paradigm, with its attendant focus on preventing unlimited liability. The majority rule finds no negligence liability for purely financial losses (the per se economic loss rule), with some jurisdictions recognizing carve-out exceptions for some form of "independent tort duty" or "special relationship" (the qualified economic loss rule). The minority rule rejects these formulations of the economic loss rule (per se and qualified), instead positing liability for negligently inflicted economic losses, conditional on particular foreseeability. Thus, the extent to which the stranger economic loss rule serves as a formidable barrier to credit card data security breach cases will depend upon the underlying state law: whether or not the state adopts the majority economic loss rule, and how it defines any exceptions thereto.

Part II turns to the contracting parties paradigm and its consideration of concurrent remedies in tort and contract and accompanying principles of deference to contract. The American Law Institute's (ALI) *Restatement (Third) of Torts: Liability for Economic Harm* has set forth a more narrowly tailored economic loss rule for parties in

19. *Id*. (noting that Visa and MasterCard Card Operating Regulations, which apply between merchants, issuer banks, and acquirer banks, specify procedures for issuer banks to make claims in the event of data breaches); *see, e.g.*, Sovereign Bank v. BJ's Wholesale Club, Inc. v. Int'l Bus. Machines Corp., 533 F.3d 162, 165 (3d Cir. 2008) ("The CISP [Cardholder Information Security Program] provisions apply to Issuers and Acquirers and include broad security requirements intended to protect Cardholder Information."); Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club Inc., 918 N.E.2d 36, 42 (Mass. 2009) ("Visa and MasterCard each issue extensive operating regulations that govern the payment processing system and their members' obligations. Every financial institution that becomes a member of Visa and MasterCard organizations must sign a contract that includes a provision that it will comply with these regulations; acquirers are also contractually obligated to ensure that their merchants comply.").

contractual privity: no liability for negligence in the negotiation or performance of a contractual duty.[20] There is, however, a significant exception for "professionals," who remain liable to their clients in tort as well as contract.[21] Several courts have viewed the credit card data security breach cases through the lens of the contracting parties paradigm, including considering the extent to which credit card processors might be considered professionals.

Having explored these two dichotomous paradigms and courts' resolution of third-party data security breach cases under each framework, Part III demonstrates how choice of paradigm can be outcome-determinative; for instance, the economic loss rule is less likely to apply under the stranger paradigm, but would bar tort liability under the contracting parties paradigm. One federal district court succinctly summed up the confounding nature of the particular type of third-party/web of contracts scenario encountered here:

> [T]he credit card industry involves a complex web of relationships involving numerous players governed by both individual contracts and exhaustive regulations promulgated by Visa and other card networks. These relationships may well create non-contractual duties between various participants in the system . . . . In addition, this web of relationships may or may not render . . . negligence claim[s] susceptible to the economic loss doctrine.[22]

Part III thus tries to pave a new road forward. Jurisdictions should not eschew entirely the contracting parties paradigm. In other words, it does not make sense to apply the stranger economic loss rule (even with exceptions) across the board regardless of the existence of contract (or contracting opportunities). Neither will it suffice, however, for jurisdictions to blithely adopt and follow the *Restatement (Third) of Torts* approach of a contractual privity economic loss rule coupled with a categorical "professionals" exception. Tort law, by forcing the internalization of externalities, plays a critical role in deterring excessively risky conduct and encouraging risk management strategies by actors and their insurers. The credit card data breach cases can be reframed in a coherent way that defers to contractual allocation of risk and responsibility but nonetheless allows tort liability to be deployed when needed to ensure the internalization of third-party

---

20. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR ECONOMIC HARM § 3 (AM. LAW INST. 2012).

21. *Id.* § 4 ("A professional is subject to liability in tort for economic loss caused by the negligent performance of an undertaking to serve a client.").

22. Banknorth, N.A. v. BJ's Wholesale Club, Inc., 394 F. Supp. 2d 283, 287 (D. Me. 2005). The court held that issues of fact as to the nature of the relationships existed and denied a motion to dismiss. *Id.* Since Maine had not yet expanded the economic loss doctrine beyond products cases, the court was hesitant to extend its reach. *Id.*

costs. Seen from a broader regulatory perspective—especially taking into account state statutory provisions relating to enforcement of private industry standards in the credit card arena—the economic loss rule functions as a boundary-policing doctrine between tort and regulation as alternative mechanisms to regulate private parties.

II. The Stranger Paradigm

Tort law's classic domain is the "stranger paradigm"—injuries inflicted on victims with whom the actor has no pre-existing contractual or special relationship. Indeed, whereas contract law deals with enforcing bargains between consenting parties, tort law allocates risks and responsibilities among strangers in society, all of whom have duties imposed *by law* to act with reasonable care towards others to avoid inflicting injuries. At its core, tort law protects physical injuries and damage to property. It does so by imposing a general duty on actors to take reasonable care to avoid physical injuries to persons and property; however, tort law traditionally imposes far more limited duties to avoid causing purely financial losses.

Courts' (as opposed to scholars') main concern in the realm of pure financial loss centers on foreseeability and the prospect of unlimited liability.[23] In the classic words of a Pennsylvania court,

> [N]egligent harm to economic advantage alone is too remote for recovery under a negligence theory. The reason a plaintiff cannot recover stems from the fact that the negligent actor has no knowledge of the contract or prospective relation and thus has no reason to foresee any harm to the plaintiff's interest.[24]

Moreover, the court reasoned:

> To allow a cause of action for negligent cause of purely economic loss would be to open the door to every person in the economic chain of the negligent person or business to bring a cause of action. Such an outstanding burden is clearly inappropriate and a danger to our economic system.[25]

The "stranger economic loss rule" posits that, as between parties with no contractual or special relationship, there is no duty to avoid negligent infliction of purely financial losses.[26] The majority posi-

23. For a critique of scholars' philosophical and economic justifications of the stranger economic loss rule, see Catherine M. Sharkey, *In Search of the Cheapest Cost Avoider: Another View of the Economic Loss Rule*, 84 U. Cin. L. Rev. (forthcoming 2017).

24. Aikens v. Baltimore & Ohio R.R. Co., 501 A.2d 277, 279 (Pa. Super. Ct. 1985).

25. *Id*.

26. *See* Dobbs, *supra* note 6, at 715 ("The first of the economic loss rules (the stranger rule) . . . is that, subject to some qualifications, a defendant owes no duty to exercise reasonable care for the pure stand-alone economic interests of strangers–that is to persons with whom the defendant has no relationship by contract, undertaking, or specific legal obligation.").

tion—illustrated by the New York Court of Appeals canonical 2001 decision in *532 Madison Avenue Gourmet Foods, Inc. v. Finlandia Center, Inc.*[27]—embraces the stranger economic loss rule, subject to a number of exceptions, including independent duty or special relationship and negligent misrepresentation.[28] The minority position—embraced by the New Jersey Supreme Court in its similarly canonical, 1985 decision *People Express Airlines, Inc. v. Consolidated Rail Corp.*[29]—rejects a per se stranger economic loss rule, and instead cabins liability for purely financial losses with a particular foreseeability constraint.[30]

The first lesson to emerge from data security breach cases is that the extent to which the stranger economic loss rule will bar recovery is highly dependent on the governing state law, which varies considerably across the United States.

A. Majority Rule of 532 Madison Ave. Gourmet

The *532 Madison Ave. Gourmet* scenario is as follows: a construction project is handled negligently; a building under construction collapses, and several surrounding blocks in a highly concentrated, commercial shopping district have to be closed.[31] A neighboring deli sues the building owner for financial losses stemming from the loss of business during the several weeks of restricted entry to the area.[32]

The New York Court of Appeals held that negligence claims asserting purely economic losses are foreclosed, absent some sort of special relationship that would warrant imposing on the defendant a duty to act with reasonable care towards those with whom he is not in a direct relationship.[33] Under the *532 Madison Ave. Gourmet* conception of the economic loss rule, courts focus on whether a direct relationship exists between the tortfeasor and the victim.[34] By embracing the stranger economic loss rule, courts seek to prevent boundless liability "to an indeterminate class of persons conceivably injured by any negligence in a defendant's act."[35]

---

27. 750 N.E.2d 1097 (N.Y. 2001).
28. *Id*. at 1099–1100.
29. 495 A.2d 107 (N.J. 1985).
30. *Id*. at 114–16.
31. *532 Madison Ave. Gourmet*, 750 N.E.2d at 1099–1100.
32. *Id*.
33. *Id*. at 1101 ("Landowners, for example, have a duty to protect tenants, patrons and invitees from foreseeable harm caused by the criminal conduct of others while they are on the premises, because the special relationship puts them in the best position to protect against the risk.").
34. *Id*. ("Absent a duty running directly to the injured person there can be no liability in damages, however careless the conduct or foreseeable the harm.").
35. *Id*.

We turn now to courts' application of the majority stranger economic loss rule to data security breach cases.

1. No Negligence Liability for Purely Financial Losses

Pennsylvania and Massachusetts have embraced fairly robust per se economic loss rules,[36] and data security breach claims decided under those states' underlying common law have not fared well.

Pennsylvania refuses to "recognize a cause of action to compensate a party suffering purely economic loss, absent any direct physical injury or property damage as a result of the negligence of another party."[37] In fashioning the economic loss rule, courts have drawn from the *Robins Dry Dock*[38] principle (which also animates the no-recovery rule in *532 Madison Ave. Gourmet*) of avoiding indeterminate liability to an indeterminate class.[39] To echo the words quoted above from the Pennsylvania Superior Court:

> To allow a cause of action for negligent cause of purely economic loss would be to open the door to every person in the economic chain of the negligent person or business to bring a cause of action. Such an outstanding burden is clearly inappropriate and a danger to our economic system.[40]

In the context of credit card data security breaches, courts have suggested that the notion of foreseeability as a limitation is stretched beyond limit when the class is defined as those whose information the bank has on file.[41]

Consider *Sovereign Bank v. BJ's Wholesale Club, Inc.*,[42] the Pennsylvania class action lawsuit stemming from a data security breach at BJ's Wholesale Club. The issuer bank sued the merchant and argued that the foreseeability of the loss of sensitive information due to lax

---

36. *See In re* Michaels Store Pin Pad Litig., 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011) (holding, under Illinois law, that "the economic loss doctrine bars the plaintiff's tort claim because the plaintiff has not suffered personal injury or property damage" and citing Massachusetts and Pennsylvania law favorably).

37. Aikens v. Baltimore & Ohio R.R. Co., 501 A.2d 277, 278 (Pa. Super. Ct. 1985); *see also* Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183, 204 (M.D. Pa. 2005) ("*Aikens*'s economic loss doctrine has been followed in subsequent cases to bar negligence claims seeking recovery for 'economic damages' or 'losses' unless there has also been physical injury either to a person or property.").

38. Robins Dry Dock & Repair Co. v. Flint, 275 U.S. 303 (1927).

39. *Id*. at 308–09; *see* 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 711 N.Y.S.2d 391, 393–94 (App. Div. 2000) (referencing *Robins Dry Dock*).

40. *Aikens*, 501 A.2d at 279.

41. *See* Pa. State Emps. Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 336 (M.D. Pa. 2005).

42. 395 F. Supp. 2d 183 (M.D. Pa. 2005), *aff'd in relevant part*, 533 F.3d 162, 175–78 (3d Cir. 2008).

data security measures should overcome the economic loss rule.[43] The federal district court, applying Pennsylvania law, disagreed, noting the resolute quality of Pennsylvania's economic loss rule, barring "negligence claims seeking recovery for economic damages or losses unless there has also been physical injury either to a person or property."[44] Moreover, the court reinforced the underlying unlimited liability rationale for the rule: "[A]s a matter of public policy . . . there would be no right of recovery in negligence for economic losses to prevent anyone 'in the economic chain' to sue so that the 'economic system' would not be burdened."[45] The Third Circuit Court of Appeals affirmed, rejecting the issuer bank's attempt "to get around the fatal limitation of the economic loss doctrine."[46]

Massachusetts embraces a similarly broad, per se economic loss rule: "[P]urely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage."[47] Courts applying Massachusetts law likewise readily dispense with data breach claims. A paradigmatic example arose in *In re TJX Cos. Retail Security Breach Litigation*,[48] in which hackers broke into the proprietary systems of TJX Companies, a group of apparel and home merchants, gaining access to the personal and financial information of over forty-five million customer accounts.[49] Plaintiffs, including issuing banks responsible for distributing debit and credit cards to their customers, sued TJX and Fifth Third Bank (the payment card processor) to recover financial losses stemming from their negligence in fail-

43. Sovereign Bank (issuer bank) issued Visa cards to cardholders who used the cards at BJ's. In turn, "BJ's retained the cardholders' information after Sovereign had approved the transactions, contrary to the operating regulations. Thereafter, third parties [hackers] obtained the cardholder information to make unauthorized purchases." *Id*. at 189–90, 204 (citations omitted).

44. *Id*. at 204. Sovereign had claimed reimbursement for the fraudulent transactions as well as expenses for issuing new cards, the loss of fees and commissions while the cards were being replaced, and loss of good will. *Id*. at 189–90.

45. *Id*. at 204 (quoting *Aikens*, 501 A.2d at 279).

46. *Pa. State Emps. Credit Union*, 533 F.3d at 176 (rejecting the issuer bank's "attempt[ ] to pirouette around the economic loss doctrine by arguing that it only applies when the plaintiff has suffered an unforeseeable loss").

47. Aldrich v. ADD Inc., 770 N.E.2d 447, 454 (Mass. 2002) (quoting FMR Corp. v. Bos. Edison Co., 613 N.E. 2d 902, 903 (Mass. 1993)); *see also* Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club Inc., 918 N.E.2d 36, 46 (Mass. 2009) ("[T]he 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.").

48. 524 F. Supp. 2d 83 (D. Mass. 2007).

49. *Id.* at 85–86.

ing to secure the cardholder data.[50] The federal district court rejected the claim, relying on Massachusetts' per se economic loss rule.[51]

Affirming the district court's decision, the First Circuit Court of Appeals reasoned that "[l]ike 'duty' and 'proximate cause,' the doctrine cabins what could otherwise be open-ended negligence liability to anyone affected by a negligent act."[52] This general concern for potentially unlimited liability permeates courts' articulation of the stranger economic loss rule, whereby, absent physical injury to persons or property, courts insist upon some independent or special relationship before allowing recovery for negligently inflicted economic losses.[53]

The premise of the per se economic loss rule—recovery for negligently inflicted physical injuries and property damage, but excluding purely financial losses—rests on a fundamental distinction between physical injury and property damage on the one hand, and financial losses on the other. Courts take it as a given that such a distinction is justified;[54] it is, however, difficult to sustain such a dividing line—particularly separating property damage from financial losses—on philo-

50. *Id*. at 86–87.

51. *Id*. at 90 (citing *Aldrich*, 770 N.E.2d at 454). Having relied upon the per se Massachusetts rule, the court then suggested a narrower application (in light of the web of contractual relationships) that "a commercial user can protect himself by seeking express contractual assurances concerning the product (and thereby perhaps paying more for the product) or by obtaining insurance against losses." *Id*. (quoting Bay State-Spray & Provincetown S.S., Inc. v. Caterpillar Tractor Co., 533 N.E.2d 1350, 1354–55 (Mass. 1989)). The court thus suggested that, in light of the web of contractual relationships, the "victims" may be the cheapest cost avoiders here; moreover, the no recovery holding might encourage victims to protect themselves via contract or else insurance. For further discussion of this rationale, see *infra* Part V.

52. *In re TJX Cos.*, 564 F.3d at 498.

53. 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 750 N.E.2d 1097, 1101 (N.Y. 2001); *accord In re* Chi. Flood Litig., 680 N.E.2d 265, 274 (Ill. 1997) (applying the economic loss rule to victims of flood alleging purely economic losses to "avoid[ ] the consequences of open-ended tort liability"); D & D Transp., Ltd. v. Interline Energy Servs., Inc., 117 P.3d 423, 428 (Wyo. 2005) (applying the economic loss rule to claims of party not in privity with defendant, noting policy of "seek[ing] to avoid the consequence of open-ended tort liability"); *see also* Ultramares Corp. v. Touche, 174 N.E. 441, 444 (N.Y. 1931) ("If liability for negligence exists, a thoughtless slip or blunder, the failure to detect a theft or forgery beneath the cover of deceptive entries, may expose [defendants] to a liability in an indeterminate amount for an indeterminate time to an indeterminate class.").

54. The Fifth Circuit Court of Appeals made a rare attempt to justify the distinction as follows:

> The bright line rule of damage to a proprietary interest, a[t] most, has the virtue of predictability with the vice of creating results in cases at its edge that are said to be "unjust" or "unfair." . . . [W]hen lines are drawn sufficiently sharp in their definitional edges to be reasonable and predictable, such differing results are the inevitable result—indeed, decisions are the desired product. . . . [I]n addition, by making results more predictable, [the rule] serves a normative function. It operates as a rule of law and allows a court to adjudicate rather than manage.

Louisiana *ex rel.* Guste v. M/V Testbank, 752 F.2d 1019, 1029 (5th Cir. 1985).

sophical or economic theories of tort law.[55] The data security breach cases push the limits of the property/financial loss divide, as plaintiff issuing banks have endeavored to withstand dismissal pursuant to the economic loss rule by arguing that the loss of use of payment cards, as a result of a breach, qualifies as physical harm to property.[56]

To date, these claims have been roundly rejected. Courts have been unwilling to equate financial loss or consequential expenditure of money to physical property damage. The Third Circuit Court of Appeals, affirming *Sovereign Bank*, feared setting a dangerous precedent that "would totally eviscerate the economic loss doctrine because any economic loss would morph into the required loss of property and thereby furnish the damages required for a negligence claim."[57] In *Pennsylvania State Employees Credit Union v. Fifth Third Bank*,[58] a case factually identical to *Sovereign Bank*, the federal district court confronted the property damage argument by requiring a "plaintiff [to] show physical damage to property, not its tangible nature, to avoid the application of the economic loss doctrine."[59] Likewise, in *In re TJX Cos.*, noting that "data can have value and the value can be lost," the First Circuit Court of Appeals nonetheless concluded that the loss of value must have been "a result of physical destruction of property" in order for a negligence claim to survive.[60] These courts' rejections stem more from a perceived need to preserve the economic loss rule, rather than grappling at a deeper level with whether the property/economic loss distinction should persist in our modern information-age society.

---

55. *See supra* note 23 and accompanying text.

56. *See, e.g.*, Pa. State Emps. Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 329–30 (M.D. Pa. 2005) (detailing plaintiffs' allegations that "the cards are tangible property and that the loss of the use of these cards, 'physical tangible items—constitutes property damage that obviates the economic loss doctrine'") (quoting Plaintiff PSECU's Brief in Opposition to BJ'S Wholesale Club's Motion to Dismiss at 20, *Pa. State Emps. Credit Union*, 398 F. Supp. 2d at 317 (No. CV-04-1554), 2005 WL 4341838); Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183, 204 (M.D. Pa. 2005) (reciting plaintiffs' allegations that they suffered "a loss of 'real and concrete' property, [their] money"); *In re TJX Cos.*, 524 F. Supp. 2d at 90 ("The issuing banks fall back on the argument that the economic loss doctrine does not, in any event, bar their negligence claim because they have incurred damage to property in that the compromised cards could no longer be used and that loss [sic] card verification codes were lost."); Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club Inc., 918 N.E.2d 36, 41 (Mass. 2009) (repeating plaintiffs' allegations that "millions of credit cards they were required to reissue constituted harm to physical property").

57. *Sovereign Bank*, 533 F.3d at 162.

58. 398 F. Supp. 2d 317.

59. *Id*. at 330; *see also Cumis*, 918 N.E.2d at 46 ("[A]s courts in other jurisdictions have observed, the question here is not whether the credit cards are tangible property, but rather the nature of the damages sought by the plaintiffs.").

60. *In re TJX Cos.*, 564 F.3d at 489.

2. Exceptions

A fairly significant number of states eschew the per se formulation of the economic loss rule and embrace instead a qualified version, whereby tort recovery for negligently inflicted economic harms is premised on an independent tort duty or some special relationship between the parties. This tort duty is some form of public duty imposed by law, not derived from contract.[61] Courts' recognition of such an independent tort duty may require an ad hoc analysis of the relationships between the parties,[62] or it may be categorically defined—such as applying to negligent misrepresentation claims.[63] Next we examine how these exceptions play out in the data breach context.

a. Independent Duty or Special Relationship

The wide array of state law formulations of the economic loss rule is on display in the multi-jurisdiction, consumer class action *In re Target Corp. Customer Data Security Breach Litigation*,[64] consolidated in the Minnesota federal district court. The court confronted the divergent economic-loss-rule doctrines across eleven different state jurisdic-

61. *See, e.g.*, A.C. Excavating v. Yacht Club II Homeowners Ass'n, 114 P.3d 862, 865–66 (Colo. 2005) (holding that a subcontractor in privity with a contractor and a developer owed an independent duty not to construct a homeowners' development negligently); Donatelli v. D.R. Strong Consulting Eng'rs, Inc., 312 P.3d 620, 627 (Wash. 2013) (allowing tort claims for purely economic loss in a construction dispute when the plaintiff can show that the defendant had a duty existing outside of the terms of the parties' contract).

62. *See, e.g.*, Davencourt at Pilgrims Landing Homeowners Ass'n v. Davencourt at Pilgrims Landing, LC, 221 P.3d 234, 244 (Utah 2009) ("'The question of whether [an independent] duty exists is a question of law' and involves the 'examination of the legal relationships between the parties, an analysis of the duties created by these relationships,' and 'policy judgments applied to relationships.'" (quoting Yazd v. Woodside Homes Corp., 143 P.3d 283, 286 (Utah 2006))).

63. *See, e.g.*, Bull v. BGK Holdings, LLC, 859 F. Supp. 2d 1238, 1243 (D.N.M. 2012) ("Common law claims of negligent and intentional misrepresentation can be examples of claims which arise from an independent and recognized duty of care."); Presnell Constr. Managers, Inc. v. EH Constr., LLC, 134 S.W.3d 575, 582 (Ky. 2004) ("[W]e agree that the tort of negligent misrepresentation defines an independent duty for which the recovery in tort for economic loss is available.").

64. 66 F. Supp. 3d 1154, 1171–76 (D. Minn. 2014). Following the court's rejection of defendant's motion to dismiss, the parties settled the claims. *See* Tamara Burns, *$10M Target Data Breach Settlement Obtains Final Approval*, TOP CLASS ACTIONS (Nov. 19, 2015), https://topclassactions.com/lawsuit-settlements/lawsuit-news/237688-target-10m-setfinal-approval/. On November 18, 2015, the Minnesota federal district court approved the $10 million class action settlement. *Id*. Approximately 110 million consumers were estimated to have had their personal information compromised by the 2013 data security breaches. *Id*. According to the judge, "In the Court's view, the settlement represents a significant victory for a class whose legal claims are as tenuous as those here." *Id*.

Target settled a separate class action lawsuit brought by financial institutions for $39 million. Ahiza Garcia, *Target Settles for $39 Million Over Data Breach*, CNN (Dec. 2, 2015, 5:48 PM), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/index.html. Target also settled separately with Visa for $67 million. *Id*.

tions.[65] The court found that members of the plaintiff consumer class, who used credit cards at a Target retail location, were not in privity with Target. The court thus employed the stranger paradigm.[66]

The court determined that Alaska, California, Illinois, Iowa, and Massachusetts all barred negligence claims arising from pure financial loss—basically deploying the per se stranger economic loss rule.[67] But other jurisdictions applied a qualified version of the rule, recognizing various exceptions to the stranger paradigm, and here, the court looked to see if the relationship weighed in favor of tort liability even in the absence of personal injury or property damage.[68] The court suggested that the near-privity, direct relationship between plaintiffs and Target created a duty. Therefore, claims made in states that recognize such an exception could not be dismissed.[69] New York, for example, allowed the independent duty exception for a privity-like relationship between Target and customers with respect to personal financial information.[70] New Hampshire, the District of Columbia, and Idaho also allowed exceptions for various kinds of special relationships.[71]

b. Negligent Misrepresentation

A corollary to the independent duty exception is the negligent misrepresentation tort, a claim that can be stated where a retailer has represented that its customers' credit card information will be protected. Some states recognize the tort as creating a type of independent duty, especially in the professional services context,[72] while

65. *In re Target Corp.*, 66. F. Supp. 3d at 1171–76.

66. *Id*. at 1171–72. The district court opinion evinces confusion on this front. Despite beginning with the view that the economic loss rule governs the boundary between tort and contract—describing the Uniform Commercial Code as the appropriate remedy for economic loss from diminished commercial expectations—the court nonetheless analyzes the situation as one in which there is no contractual privity between Target and the consumer class. *Id*. Indeed, although deploying the stranger paradigm, the court nonetheless cites third-party or web of contracts cases for support. *Id*. Moreover, the defendant chose not to argue that the economic loss rule should apply in eight states because those states bar negligence claims only between contracting parties. *Id*.

67. *Id.* at 1172–74.

68. *Id*. at 1172.

69. *Id*. at 1175 (analyzing New York law).

70. *Id*. The court stated that plaintiffs allege Target had "a quasi-contractual, privity-like relationship with respect to their personal financial information." *Id*. The court relied on a New York case that takes a stranger approach, beginning with question of duty, and finding that because of the relationship between the parties there was a duty to protect plaintiffs from economic losses. *See In re* Facebook, Inc., IPO Sec. & Derivative Litig., 986 F. Supp. 2d 428, 460–61 (S.D.N.Y. 2013).

71. *In re Target Corp.*, 66 F. Supp. 3d at 1172–75.

72. *See, e.g.*, Level 3 Commc'ns, LLC v. Liebert Corp., 535 F.3d 1146, 1163 (10th Cir. 2008) ("Colorado tort law, whatever else it may or may not require by way of accuracy in describing

others recognize the tort as a stand-alone exception to the economic loss rule.[73]

Data breach plaintiffs have invoked negligent misrepresentation claims to avoid the economic loss rule with varying degrees of success. Not surprisingly, jurisdictions such as Pennsylvania, which have embraced a robust per se economic loss rule, have narrowly construed the negligent misrepresentation carve-out.

In *Sovereign Bank*, the Third Circuit Court of Appeals (applying Pennsylvania law) rejected plaintiffs' move to shoehorn liability into the negligent misrepresentation mold, which the court described narrowly as a "doctrine to allow a commercial plaintiff recourse from an 'expert supplier of information' with whom the plaintiff has no contractual relationship, when the plaintiff has relied on that person's 'special expertise' and the 'supplier negligently misrepresents the information to another in privity.'"[74] As the court recognized, many other courts recognize claims of third-party negligent misrepresentation in situations when the very nature of the work engaged in by

commercial goods, clearly imposes a duty of reasonable care or competence in obtaining or communicating the information.") (quoting RESTATEMENT (SECOND) OF TORTS § 552(1) (AM. LAW INST. 1976)); Donatelli v. D.R. Strong Consulting Eng'rs, Inc., 312 P.3d 620, 625 (Wash. 2013) (en banc) ("[T]he duty to avoid misrepresentations that induce a party to enter into a contract arises independently of the contract.").

73. *See, e.g.*, Fireman's Fund Ins. Co. v. SEC Donahue, Inc., 679 N.E.2d 1197, 1199 (Ill. 1997) (recognizing an exception to Illinois' economic loss rule "where the plaintiff's damages are proximately caused by a negligent misrepresentation by a defendant in the business of supplying information for the guidance of others in their business transactions") (citing Moorman Mfg. Co. v. Nat'l Tank Co., 435 N.E.2d 443, 452 (Ill. 1982)); Van Sickle Const. Co. v. Wachovia Commercial Mortg., Inc. 783 N.W.2d 684, 691–92 (Iowa 2010) (stating that in Iowa, "negligent misrepresentation has always been understood as an economic tort allowing for the recovery of purely economic losses"); RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR ECONOMIC HARM § 5 (AM. LAW INST. 2012); RESTATEMENT (SECOND) OF TORTS § 552 (AM. LAW INST. 1976) (recognizing liability for pecuniary loss in cases of negligent misrepresentation).

74. Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 177 (3d Cir. 2008) (quoting Bilt-Rite Contractors, Inc. v. Architectural Studio, 866 A.2d 270, 286 (Pa. 2005)). Plaintiffs relied heavily on a case involving a general construction contractor that relied in its winning bid on design specifications provided by the defendant architecture firm and sued the firm when they discovered that the construction would require "special construction means, methods and design tables [not provided for in the design], resulting in substantially increased construction costs." *Bilt-Rite Contractors*, 886 A.2d at 272. The court in *Bilt-Rite* had to determine whether a negligent misrepresentation action could be maintained against the architecture firm where there was no privity between the parties, but there was foreseeable reliance on the information supplied by the architect. *Id*. The court, adopting § 552 of the *Restatement (Second) of Torts*, concluded that such an action could be maintained. *Id*. at 272–73. In part, it was persuaded that § 552 "reflect[s] modern business realities" and "merely recognizes that it is reasonable to hold [design] professionals to a traditional duty of care for foreseeable harm." *Id*. at 286. As such, it permitted the negligent misrepresentation action to overcome the economic loss rule because it was foreseeable that Bilt-Rite would be harmed through its justifiable reliance on the architecture firm's negligently supplied information. *Id*. at 288.

professionals—including architects, lawyers, and accountants—potentially creates a duty to others that operates regardless of the existence of privity of contract. The court concluded that while it may be reasonable to argue that Sovereign Bank relied on BJ's representation to protect its customers' sensitive information, BJ's did not hold itself out either as a professional or an "expert supplier of information" such that it would be liable for the breach of some independent duty owed to Sovereign Bank.[75]

In a recent data breach action addressing traditional third-party negligent misrepresentation claims asserted in an effort to evade Pennsylvania's economic loss rule, a Pennsylvania federal district court likewise barred the claim.[76] The court elaborated on data breach cases as appropriate contexts for the economic loss rule:

> [I]n this era, where the threat of data breaches by unknown third parties is omnipresent, regardless of what preventative measures are taken, the potential disparity between the degree of a defendant's fault and the damages to be recovered could be immensely disproportionate, resulting in drastic implications for defendants named in lawsuits as well as our economic system at large.[77]

Thus, although Pennsylvania does recognize the tort of negligent misrepresentation in certain contexts, it does not in the context of a data security breach.

Nevada, however, has recognized negligent misrepresentation claims in the data breach context. In *In re Zappos.com*,[78] a lawsuit arose after a 2012 data breach of Zappos.com, an online shoe and clothing retailer.[79] Hackers gained access to Zappos customer servers containing personal information of about twenty-four million Zappos customers.[80]

The court, recognizing that Nevada's economic loss rule would bar the plaintiffs' negligence claims, treated the negligence claims as negligent misrepresentation claims.[81] Nevada recognizes negligent misrep-

---

75. *Sovereign Bank*, 533 F.3d at 177–78.

76. *See* Longenecker-Wells v. BeneCard Servs., Inc., No. 15-CV-00422, 2015 WL 5576753, at *7 (M.D. Pa. Sept. 22, 2015), *aff'd*, 658 F. App'x 659 (3d Cir. 2016).

77. *Id*. at *6.

78. *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., No. 12-cv-00325-RCJ-VPC, 2013 WL 4830497 (D. Nev. Sept. 9, 2013).

79. *Id*. at *1–4.

80. David Goldman, *Zappos Hacked, 24 Million Accounts Accessed*, CNN (Jan. 16, 2012, 11:33 AM), http://money.cnn.com/2012/01/16/technology/zappos_hack/.

81. The court noted that the interaction between customers and the website resulted in a contract for the sale of goods that was not alleged to have been breached by the data loss. *In re Zappos.com*, 2013 WL 4830497, at *3. However, the website also set forth "unilateral statements of fact as to the safety of customers' data" which could be the basis of a negligent misrepresentation tort claim if made negligently. *Id*. Thus, the court asked not whether the data security was

resentation as an exception to the economic loss rule because without such liability "the law would not exert significant financial pressures to avoid such negligence," including "negligent misstatements about financial matters."[82] As a means to effectuate that policy, the *Zappos* court noted that if plaintiffs have an opportunity to incorporate "a particular standard of performance" into a contract, then the duties the parties owe to each other are dictated by the contractual agreement.[83] In this case, however, the court found no evidence that the agreements between the parties constituted a contractual scheme that would "exert significant financial pressure" on Zappos to avoid making misrepresentations to its customers.[84] Consequently, the court concluded that the economic loss doctrine did not preclude claims of negligent misrepresentation in this case and permitted the plaintiffs to amend their claims.[85]

B. Minority Rule of People Express

The stranger economic loss rule (with varying degrees of qualifications for recognizing independent tort duties) has gained a foothold in jurisdictions across the United States. But the New Jersey Supreme Court—long a "leader in expanding tort liability"[86]—resisted the rule in *People Express*.[87] In that case, an airline sued the defendant rail yard owner for business interruption losses after a volatile chemical caught fire in the defendant's rail yard, located adjacent to Newark

---

negligent, but rather whether the promise that the data would be protected was negligent. *See id*.

82. *Id.* at *4 (quoting Halcrow, Inc. v. Eighth Judicial Dist. Court, 302 P.3d 1148, 1153 (Nev. 2013)).

83. *Id*. (quoting *Halcrow*, 302 P.3d at 1153).

84. *Id*. (quoting *Halcrow*, 302 P.3d at 1153). The court thus suggested that negligent misrepresentation is an exception to the economic loss rule only where there are not detailed and negotiated contracts. In other words, it is an exception to the stranger economic loss rule, but would not necessarily apply under the contracting parties paradigm.

85. *Id*. at *4 & n.2 (allowing the plaintiffs to amend their complaint given that "negligently misstat[ing] the safety of Plaintiff's financial information" was not precluded by Nevada's economic loss rule).

86. *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., No. H-10-171, 2011 WL 1232352, at *21 (S.D. Tex. Mar. 31, 2011) (quoting Hakimoglu v. Trump, 70 F.3d 291, 295 (3d Cir. 1995)).

87. People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 116 (N.J. 1985). The *Restatement (Third) of Torts: Liability for Economic Harm* embraces the stranger economic loss rule, as elaborated in *532 Madison Ave. Gourmet* and *Robins v. Dry Dock*. *See* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR ECON. HARM § 7 (AM. LAW INST. 2014). The Reporter's Note seeks to marginalize the *People Express* minority position. *Id*. at cmt. a ("Contrary positions have been taken only occasionally in the case law." (citing *People Express* and Mattingly v. Sheldon Jackson Coll., 743 P.2d 356 (Alaska 1987))).

Airport.[88] Due to the chemical spill and risk of fire, an evacuation of a one-mile radius was ordered.[89] The airport terminal, located within the one-mile radius, was shut down for twelve hours, forcing the airline to cancel flights and preventing its employees from booking flights.[90]

The New Jersey Supreme Court roundly rejected the economic loss rule, reasoning that the traditional reasons for prohibiting recovery for economic losses (i.e., fears of unlimited liability and fraudulent claims) did not justify a per se bar on recovery.[91] The court proposed a rule that would recognize a limited duty owed to "particular plaintiffs or plaintiffs comprising an identifiable class with respect to whom defendant knows or has reason to know are likely to suffer such damages from its conduct."[92] In other words, the duty to prevent financial losses hinged on the foreseeability of damages. Nonetheless, the court conceded that "the courts will be required to 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."[93] The court concluded that the business interruption losses suffered by the airline were, or should have been, foreseeable to the defendant.[94] Specifically, the court reasoned that, given the close proximity of the terminal and the airline to the freight yard, the obvious nature of plaintiff's operations, and particular foreseeability of economic losses resulting from an accident and evacuation—coupled with the defendants' knowledge of the volatile properties of the chemicals and the existence of an emergency response plan calling for an evacuation—the plaintiff's economic losses, including lost profits, should be recoverable.[95]

The *People Express* rule was front and center in the credit card data breach at issue in *Lone Star National Bank, N.A. v. Heartland Pay-*

88. *People Express*, 495 A.2d at 108.

89. *Id*.

90. *Id*.

91. *Id*. at 109–12.

92. *Id*. at 116. In *532 Madison Ave. Gourmet*, the New York Court of Appeals simultaneously distinguished and rejected the *People Express* ruling. 532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc., 750 N.E.2d 1097, 1101, 1103 (N.Y. 2001). The court described a special relationship as giving rise to a duty to protect the plaintiff against the risk of harm because it "puts [defendant] in the best position to protect against the risk." *Id*. This is distinct from the *People Express* "particular foreseeability" standard because it does not apply to the general public. *Id*. at 1102. As the New York Court of Appeals explained: "[W]herever the line is drawn, invariably it cuts off liability to persons who foreseeably might be plaintiffs." *Id*. at 1103.

93. *People Express*, 495 A.2d at 116.

94. *Id*. at 118.

95. *Id*.

ment Systems.[96] In 2009, Heartland Payment Systems, an electronic payment processor, discovered that it had been hacked and millions of credit card numbers within its database had been compromised.[97] Issuer banks asserted that Heartland was negligent in failing to comply with the Payment Card Industry Data Security Standards, a set of regulations and guidelines developed by payment card networks such as Visa and MasterCard "to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally."[98] The issuer banks asserted purely economic losses in the form of fraudulent charges and the cost of reissuing new credit cards.[99] In a consolidated multi-district litigation, a Texas federal district court held that the economic loss rule barred the claims.[100]

The Fifth Circuit Court of Appeals reversed, holding that "under New Jersey law, the economic loss doctrine does not bar tort recovery where the defendant causes an identifiable class of plaintiffs to which it owes a duty of care to suffer economic loss that does not result in *boundless liability*."[101] The court did not have difficulty finding that the issuer banks constituted an "identifiable class."[102] As the court explained, "Heartland had reason to foresee the Issuer Banks would be the entities to suffer economic losses were Heartland negligent. The 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."[103] Nor, the court reasoned, would Heartland be "exposed to 'boundless liability,' but rather to the reasonable amount of loss from a limited number of entities."[104] Moreover, "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.'"[105]

---

96. 729 F.3d 421, 424–26 (5th Cir. 2013).

97. *See In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 573 (S.D. Tex. 2011), *rev'd in part*, Lone Star Nat'l Bank v. Heartland Payment Sys., 729 F.3d 421 (5th Cir. 2013).

98. *Id*. at 575; *see* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES 5 (2016), https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf.

99. *In re Heartland Payment Sys.*, 834 F. Supp. 2d at 588–89.

100. *Id*. at 590. For discussion of the district court's decision, see *infra* notes 138–48 and accompanying text. I have deferred discussion because the district court framed the case within the contracting parties paradigm—not the stranger paradigm.

101. *Lone Star*, 729 F.3d at 424 (emphasis added).

102. *Id*. at 426.

103. *Id*. (citation omitted) (citing People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 116 (N.J. 1985)).

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

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

III. The Contracting Parties Paradigm

Moving from the stranger paradigm to the contracting parties paradigm involves a significant analytical shift. No longer is the overriding concern the threat of unlimited or disproportionate liability; indeed, the nature of privity de facto limits the parties whose interests might be impacted. The paramount issue facing courts is whether to recognize concurrent remedies in tort and contract; stated differently, in what circumstances should there be a tort duty imposed by law, notwithstanding the voluntary contractual arrangements to which the parties have agreed. On the whole, courts that apply the contracting parties paradigm tend to favor resolution of the conflict under the terms of parties' existing contractual obligations, resisting recognition of negligence claims asserting purely economic loss.

The ALI's *Restatement (Third) of Torts: Liability for Economic Harm* has articulated a contractual privity economic loss rule, barring tort recovery for negligently inflicted economic harms arising between contracting parties.[106] The *Restatement (Third) of Torts* (and all jurisdictions that have adopted such a rule) nonetheless carves out an exception for certain "professionals," who remain subject to concurrent liability in tort and contract.[107]

Several courts have applied the contracting parties paradigm (as opposed to the stranger paradigm) to credit card data security breach cases. Recall that the prototypical credit card data breach claim arises between an issuing bank (those that issue credit and debit cards to customers) and the breaching organization (usually a merchant or payment card processor). Both plaintiffs and defendants have a contractual relationship with a third-party payment card network such as Visa or MasterCard. To place these cases within the contracting parties paradigm, courts characterize this chain of privity as creating a complex regime of (typically) sophisticated parties that militates deference to contract, especially because Visa and MasterCard regula-

106. Restatement (Third) of Torts: Liability for Economic Harm § 3 (Am. Law Inst. 2012). The *Restatement (Third) of Torts* extends the contractual economic loss rule to claims of negligent misrepresentation as well. *Id*. § 5(5) (recommending no liability for negligent misrepresentations "made in the course of negotiating or performing a contract between the parties"). *Restatement (Second) of Torts* § 552 imposed no similar restriction and would seemingly allow for claims of negligent misrepresentation even among contracting parties. Restatement (Second) of Torts § 552 (Am. Law Inst. 1976).

107. Restatement (Third) of Torts: Liability for Economic Harm § 4; *see id*. § 4 cmt. b ("Lawyers, doctors, and accountants are invariably regarded by courts as professionals; insurance agents and architects are examples of additional parties this Restatement would so recognize, whereas construction contractors and tradesmen are on the other side of the line.").

tions provide for redress in the event of a data breach affecting members of the network.[108]

A. No Negligence Liability Between Contracting Parties

The contractual privity economic loss rule holds generally that there can be no recovery for purely economic losses when parties have had the opportunity to allocate risk according to the terms of their contractual relationship.[109] In principle, this means that when a contractual remedy is apparent between the parties, courts will invoke the economic loss rule as a means to channel claims for purely economic losses away from tort and toward contract law.

Occasionally, though privity between the parties may not be apparent, courts may nonetheless find that the parties operate in a complex web of relationships that create a privity-like situation.[110] Thus, though the parties may appear to be strangers, their presence in an

108. *See, e.g.*, *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 588 (S.D. Tex. 2011) ("By participating in the Visa and MasterCard networks, the Financial Institution Plaintiffs entered into the web of contractual relationships that included not only issuer and acquirer banks but also third-party businesses, such as [Defendant] Heartland, that process transactions for network members."), *rev'd in part*, Lone Star Nat'l Bank v. Heartland Payment Sys., 729 F.3d 421 (5th Cir. 2013); *see also* Banknorth, N.A. v. BJ's Wholesale Club, Inc., 394 F. Supp. 2d 283, 287 (D. Me. 2005) ("[T]he credit card industry involves a complex web of relationships involving numerous players governed by both individual contracts and exhaustive regulations promulgated by Visa and other card networks. These relationships may well create non-contractual duties between various participants in the system . . . [and] may or may not render Plaintiff's negligence claim susceptible to the economic loss doctrine.").

109. This version of the economic loss rule originated in the products liability context and then courts extended it outward to cover services as well as products and then to additional consensual exchanges. *See* Catherine M. Sharkey, *The Remains of the Citadel (Economic Loss Rule in Products Cases)*, 100 MINN. L. REV. 1845 (2016) (discussing the rule's origins in products liability); *see, e.g.*, E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 871 (1986) ("When a product injures only itself the reasons for imposing a tort duty are weak and those for leaving the party to its contractual remedies are strong."); Ass'n of Apartment Owners of Newtown Meadows *ex rel.* Bd. of Dirs. v. Venture 15, Inc., 167 P.3d 225, 279 (Haw. 2007); Indianapolis-Marion Cty. Pub. Library v. Charlier Clark & Linard, P.C., 929 N.E.2d 722, 729 (Ind. 2010) ("[T]he economic loss rule reflects that the resolution of liability for purely economic loss caused by negligence is more appropriately determined by commercial rather than tort law."); Giddings & Lewis, Inc. v. Indus. Risk Insurers, 348 S.W.3d 729, 738 (Ky. 2011) (noting that the economic loss rule "recognizes that economic losses, in essence, deprive the purchaser of the benefit of his bargain and that such losses are best addressed by the parties' contract and relevant provisions of Article 2 of the Uniform Commercial Code"); Berschauer/Phillips Constr. Co. v. Seattle Sch. Dist. No. 1, 881 P.2d 986, 992 (Wash. 1994) (en banc) ("If tort and contract remedies were allowed to overlap, certainty and predictability in allocating risk would decrease and impede future business activity."); Excel Const., Inc. v. HKM Eng'g, Inc., 228 P.3d 40, 45 (Wyo. 2010) ("The economic loss rule is founded on the theory that parties to a contract may allocate their risks by agreement and do not need the special protections of tort law to recover for damages caused by a breach of the contract.") (citations omitted).

110. *See, e.g.*, Annett Holdings, Inc. v. Kum & Go, L.C., 801 N.W.2d 499, 505 (Iowa 2011).

"inter-connected web of relationships within the market"[111] may draw the parties into a consensual framework. Accordingly, courts look to apply a version of the rule that is grounded in the reasons and justifications for deference to contract: to encourage allocation of risk through contract and to guard against remedying disappointed commercial expectations in tort.[112]

Such a rationale has been applied to several data breach cases, where courts have recognized that payment card issuers, merchants, acquirer banks, and processors all operate in a complex payment card ecosystem. A prime example is *Annett Holdings, Inc. v. Kum & Go, L.C.*[113] Annett and Kum & Go were not in direct privity, but their relationship existed through a web of contracts connecting them with a common third party, the credit card issuer Comdata.[114] A trucking company's employee used a card issued by the company (a subsidiary of Annett) to make unauthorized purchases at a gas station (Kum & Go).[115] The credit card network, Comdata, had rules covering risk allocation for fraud charges similar to Visa and MasterCard, whereby the issuing bank and trucking company were required to bear the losses.[116] The trucking company sued the gas station, which was not in privity with the trucking company, but contracted with the company's credit card network.

The court held that these relationships constituted enough of a contract-like arrangement to preclude tort-based liability: "When two parties have a contractual relationship, the economic loss rule prevents one party from bringing a negligence action against the other over the first party's defeated expectations—a subject matter the parties can be presumed to have allocated between themselves in their contract."[117] The court applied this approach to the web of contracts, noting that "the doctrine is by no means limited to the situation where the plaintiff and the defendant are in direct contractual privity."[118] The court reasoned:

---

111. *In re* Syngenta AG MIR 162 Corn Litig., 131 F. Supp. 3d 1177, 1191 (D. Kan. 2015).

112. *See, e.g.*, Mark P. Gergen, *The Ambit of Negligence Liability for Pure Economic Loss*, 48 ARIZ. L. REV. 749, 764–65 (2006) (noting that liability has been precluded when the "[plaintiff] could have obtained redress for the harm from the actor by contract with the actor or through a chain of contracts reaching back to the actor").

113. 801 N.W.2d 499.

114. *Id*. at 501.

115. *Id*.

116. *Id*. at 502.

117. *Id*. at 503.

118. *Id.* at 504. The court invoked "the stranger economic loss rule" to make this point. *Id*. And it then analyzed the case through the stranger paradigm lens, highlighting the unlimited liability rationale: Lacking direct privity, economic loss must still be contained because "'[i]n a

> When parties enter into a chain of contracts, even if the two parties at issue have not actually entered into an agreement with each other, courts have applied the "contractual economic loss rule" to bar tort claims for economic loss, on the theory that tort law should not supplant a consensual network of contracts.[119]

Applied to the case before it, the court reasoned that each party could allocate the risk ex ante through the web of contracts and, as such, "it is difficult to see why a tort remedy is needed here."[120] Moreover, according to the court, the trucking company "contracted to assume certain risks of financial loss and had the ability to minimize these risks."[121]

The Massachusetts Supreme Judicial Court likewise stood firm against the encroachment of tort into contract in *Cumis Insurance Society, Inc. v. BJ's Wholesale Club, Inc.*,[122] a case involving the same data breach of BJ's Wholesale Club discussed above, whereby hackers gained access to over nine million credit card numbers stored by the merchant.[123] The plaintiff credit unions that issued the compromised credit cards suffered financial losses from cancelling and reissuing credit cards to their affected customers. They brought claims against BJ's and Fifth Third (the credit card processor) for negligence and negligent misrepresentation.[124] Applying Massachusetts' per se economic loss rule, the court readily dispatched the negligence claim.[125]

---

complex society such as ours, economic reverberations travel quickly and widely, resulting in potentially limitless liability.'" *Id*. The court characterized Annett's claim thusly: "It is a remote economic loss claim . . . but with the additional twist that this case does not even involve an *initial* personal injury or damage to property." *Id*. The court then turned to analyzing the case under the contracting parties paradigm—and it is this alternative framework that I highlight in the text above.

Note, however, that the dissent applies the stranger paradigm exclusively—and reaches the opposite conclusion. *See id*. at 508, 511 (Wiggins, J., dissenting) ("Allowing the claim against Kum & Go to proceed will not result in a flood of litigation, speculative damages, or thwart any of the other rationales commonly asserted in association with the economic loss rule."). Here is an example of the confusion that arises when the stranger paradigm, based on unlimited liability concerns, is applied instead of the contracting parties paradigm, which focuses on delineating the border between tort and contract claims. For further discussion, see *infra* Sections IV.B–C.

119. *Annett Holdings*, 801 N.W.2d at 504.

120. *Id*. at 505.

121. *Id*. ("Annett had the capacity to prevent fraudulent or unauthorized use by its employee: Its subsidiary TMC received a daily report of [its employee's] transactions, and as soon as a new fuel manager took over, that person noticed the suspicious activity immediately."). Here, the court seemed to embrace a cheapest cost avoider rationale—to which I will return.

122. 918 N.E.2d 36 (Mass. 2009).

123. *Id*. at 39.

124. *Id*. at 40. The plaintiffs also brought claims for breach of contract as third-party beneficiaries, fraud, and various violations of consumer protection statutes. *Id*.

125. *Id*. at 46–47 (affirming the lower court's determination that "the plaintiffs suffered only economic harm due to the theft of the credit card account information, and therefore that the economic loss doctrine barred recovery on their negligence claims").

In further rejecting the misrepresentation claim, the court held that "failure to perform a contractual duty [here, to comply with regulations regarding data storage] does not give rise to a tort claim for negligent misrepresentation."[126] The court clearly viewed the tort claims as an effort to circumvent the web of contracts, and the court was resolute in maintaining that "[p]laintiffs who are unable to prevail on their contract claims may not repackage the same claims under tort law."[127]

B. Professionals/Special Relationship Exception

The contracting-parties economic loss rule recognizes an exception for professionals[128] and possibly other special relationships between the parties arising independent of contract.[129] Some jurisdictions may even recognize a professional services situation as creating a special relationship between the parties.[130] Underlying these exceptions is the idea that, although parties to a contract are expected to allocate risk amongst themselves, there are external duties (separate and apart from contractual ones) that may occasionally be imposed on professionals, expert dealers in certain types of information, among others.

In data breach cases between contracting parties (or parties operating amidst a web of contractual relations), plaintiffs have attempted to

126. *Id*. at 49. The court called attention to the governing Visa and MasterCard operating regulations that required the defendant retailer and acquiring bank to take steps to protect cardholder information. *Id*.

127. *Id*.

128. *See, e.g.*, Indianapolis-Marion Cty. Pub. Library v. Charlier Clark & Linard, P.C., 929 N.E.2d 722, 736 (Ind. 2010) ("Indiana courts should recognize that the rule is a *general* rule and be open to appropriate exceptions, such as . . . lawyer malpractice."); Annett Holdings, Inc. v. Kum & Go, L.C., 801 N.W.2d 499, 504 (Iowa 2011) ("[P]urely economic losses are recoverable in actions asserting claims of professional negligence against attorneys and accountants.") (citing Van Sickle Constr. Co. v. Wachovia Commercial Mortg., 783 N.W.2d 684, 692 n.5 (Iowa 2010)); Plourde Sand & Gravel Co. v. JGI E., Inc., 917 A.2d 1250, 1255 (N.H. 2007) (noting that New Hampshire has applied a special relationship exception to attorneys and insurance investigators); Tommy L. Griffin Plumbing & Heating Co. v. Jordan, Jones & Goulding, Inc., 463 S.E.2d 85, 89 (S.C. 1995) ("[W]e have long held lawyers and accountants liable in tort for malpractice. . . . These professionals, however, owe a duty to the client and sometimes to third parties which arises separate and distinct from the contract for services."); LAN/STV v. Martin K. Eby Constr. Co., 435 S.W.3d 234, 243–44 (Tex. 2014) ("Professional malpractice cases are an exception [to Texas' economic loss] rule. A client can recover purely economic losses from a negligent lawyer, regardless of whether the lawyer and client have a contract.").

129. *See, e.g.*, Gulfstream Aerospace Servs. Corp. v. U.S. Aviation Underwriters, Inc., 635 S.E.2d 38, 45 (Ga. Ct. App. 2006) ("There is an exception to [the economic loss rule] if 'special circumstances' exist, such as where a 'special relationship between the parties' supporting the imposition of an independent duty of care regardless of the parties' contractual relationship.").

130. *See* EBWS, LLC v. Britly Corp., 928 A.2d 497, 507 (Vt. 2007) ("Purely economic losses may be recoverable in professional services cases because the parties have a special relationship, which creates a duty of care independent of contract obligations.").

push the boundaries of the "professionals" or "special relationship" exception. A Pennsylvania federal court resisted such efforts in *Enslin v. Coca-Cola Co.*[131] when it refused to recognize an extra-contractual special relationship between an employer and employee. *Enslin* dealt with the theft of fifty-five laptops containing the personal information of over 74,000 Coca-Cola employees.[132] Following the breach, plaintiffs sued Coca-Cola for negligence leading to fraudulent charges, resulting in account closures and identity theft.[133]

Because the parties were subject to an "arms-length business contract," the court applied the economic loss rule in order to maintain a boundary between contract and tort.[134] The court reasoned that "tort law is not intended to compensate parties for losses suffered as a result of a breach of duties assumed only by agreement."[135] Nor was the court persuaded that any "special relationship" exception applied. According to the court, to meet the high threshold for this exception, "courts must ask 'whether the relationship goes beyond mere reliance on superior skill, and into a relationship characterized by overmastering influence on one side or weakness, dependence, or trust, justifiably reposed on the other side.'"[136] The court concluded that there was no significant imbalance of power between the parties that would justify the recognition of any such special relationship.

IV. Economic Loss Rule for Data Breach Reconsidered

Third-party cases—of which the data breach cases are a prime example—do not fit squarely within either the stranger or the contracting parties paradigms, and yet the *choice of paradigm* may be outcome determinative, even more so than whether the jurisdiction adopts the majority (*532 Madison Ave. Gourmet*) or minority (*People Express*) position on the stranger economic loss rule. Moreover, courts exhibit a kind of paradigm confusion in this area, often applying the stranger paradigm to situations for which it is ill-suited.

In the face of this paradigm confusion—or at a minimum lack of consensus—this Article takes up the challenge to consider a deeper

131. 136 F. Supp. 3d 654, 672 (E.D. Pa. 2015).

132. *Id*. at 659.

133. *Id*. at 660.

134. *Id*. at 673 (quoting Valley Forge Convention & Visitors v. Visitor's Servs., Inc., 28 F. Supp. 2d 947, 953 (E.D. Pa. 1998)) ("If parties to routine arms-length commercial contracts for the provision of needed goods or services were held to have a 'special relationship,' virtually every breach of such a contract would support a tort claim.").

135. *Id.* at 656.

136. *Id*. at 672–73 (quoting My Space Preschool & Nursery, Inc. v. Capitol Indem. Corp., No. 14-2826, 2015 WL 1185959, at *10 (E.D. Pa. Mar. 13, 2015)).

conceptual or theoretical way to think about the role for tort liability in data breach cases. This Article insists that the contracting parties paradigm remains relevant; however, it resists mechanical application of the contractual privity economic loss rule. Rather, against the backdrop of the contracting parties paradigm, it contends that courts should inquire whether tort liability is nonetheless justified, as a result of spillovers or externalities onto third parties. In so doing, courts will appropriately be in search of the cheapest cost avoider for imposition of liability. In the course of that search, the existence of contract as the chosen method of allocation of risk and responsibility between the parties should be a significant factor, but one that could be outweighed in contexts where such arrangements externalize significant risk onto hapless third parties.

A. Choice of Paradigm Matters

The *Lone Star* case presents the choice of paradigm in stark relief. The Fifth Circuit Court of Appeals applied the "stranger paradigm," resting its holding on New Jersey's *People Express* rejection of the stranger economic loss rule, and thus held that the tort claims should proceed.[137] In sharp contrast, the Texas federal district court below, in *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litigation*,[138] framed the case within the "contracting parties paradigm," leading the court to reject the financial institution plaintiffs' claims, finding they were better resolved according to the network of contracts that governed the payment card industry.[139] Significantly,

137. Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 426 (5th Cir. 2013). For discussion, see *supra* text accompanying notes 96–105.

138. No. H-10-171, 2011 WL 1232352 (S.D. Tex. Mar. 31, 2011).

139. *Id*. at *21–25. Defendants in subsequent data breach cases have relied on *In re Heartland* to justify dismissal on the basis of a contractual privity economic loss rule. *See, e.g.*, Defendants' Memorandum of Law in Support of Motion to Stay Discovery at 13–14, *In re* Target Corp. Customer Data Sec. Breach Litig., No. 14-2522 (PAM/JJK), 2014 WL 10520602 (D. Minn. July 3, 2014) ("MasterCard and Visa have published detailed regulations that are designed to determine *through contract* how costs will be allocated amongst issuing banks such as the Financial Institution Plaintiffs and (through their acquiring banks) merchants such as Target in the event of a payment card breach."); *see also* Appellee Silverpop Sys., Inc.'s Brief at 34 n.93, Silverpop Sys., Inc. v. Leading Mktg. Techs., No. 14-10899-FF, 2014 WL 2557621 (11th Cir. May 27, 2014); Memorandum of Points & Authorities in Support of Defendants' Motion to Dismiss First Amended Consol. Class Action Complaint at n.18, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., No. 11-MD-02258, 2013 WL 664723 (S.D. Cal. Feb. 12, 2013); Defendant Global Payment Inc.'s Reply in Support of Motion to Dismiss First Amended Complaint, Willingham v. Global Payments Inc., No. 12-cv-01157-RWS-JFK, 2012 WL 12077131, at *19 (N.D. Ga. Oct. 22, 2012); Defendant Heartland Payment Sys., Inc.'s Memorandum of Law in Support of its Motion to Dismiss, Fielder v. Penn Station, Inc., No. 12-CV-02166-CAB, 2012 WL 6148764, at n.2 (N.D. Ohio Aug. 30, 2012). Defendants have also cited *In re Heartland* to support dismissal of the issuing banks' implied contract claims. *See, e.g.*, Defendant SAIC's Memorandum in

the district court reasoned that "it is inappropriate to create tort duties between sophisticated businesses that allocate risks through contract."[140] More specifically, the court explained the "web of contractual relations" entered by plaintiff "included not only issuer and acquirer banks but also third-party businesses, such as Heartland, that process transactions for network members."[141] The acquirer bank contracted with Heartland Payment Systems, a payment card processor and target of the hack, "to process Visa and MasterCard credit-card transactions sent to them by participating merchants."[142] The contractual terms between the acquirer banks and Heartland Payment Systems incorporated the regulations set forth by Visa and MasterCard (by mandate of Visa and MasterCard).[143] These industry security standards are known as Payment Card Industry Data Security Standards (PCI-DSS).[144]

Support of Its Motion to Dismiss the Consol. Amended Complaint, *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., No. 12-mc-347 (RLW), 2012 WL 7008506, at *54 n.35 (D.D.C. Nov. 15, 2012) (noting that the plaintiffs in the case alleged "at most an indirect relationship with Heartland through Heartland's processing of transactions made with payment cards that they issued" (quoting *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 582–83 (S.D. Tex. 2011), *rev'd in part*, Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 426 (5th Cir. 2013))).

140. *In re Heartland*, 2011 WL 1232352, at *23. The district court did conclude that, under *People Express*, the issuer bank plaintiffs were particularly foreseeable. *Id*. ("The financial institutions participating are identifiable, and the kinds of damages alleged—stemming primarily from card replacement and charging of fraudulent transactions—are straightforward. The complaint also suggests that the defendants should have been aware of the possibility of a 'hacker.'"). But, according to the court, "[m]eeting the foreseeability test under *People Express* is necessary but not sufficient under New Jersey law." *Id.* The court then turned to an analysis of the contractual relationships. *Id.* at *23–24.

141. *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 588 (S.D. Tex. 2011).

142. *In re Heartland*, 2011 WL 1232352, at *3.

143. *In re Heartland Payment Sys*., 834 F. Supp. 2d at 575 (noting that Visa and MasterCard networks "require the banks they contract with to impose these regulations on the merchants who submit transactions for processing and on the entities that process the transactions").

144. *See* PCI SEC. STANDARDS COUNCIL, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Security Standard* (June 2016), https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1486264255400. The PCI-DSS consists of twelve basic requirements:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.

The PCI-DSS played a major role in the court's reliance on the contracting parties paradigm. According to the court, because there is a dispute resolution procedure in place for noncompliance, any entity subject to network regulations is governed by those regulations, not tort. The court was convinced that the parties' separate relations with Visa and MasterCard created a viable avenue in contract by which the issuer banks could seek redress from the acquirer banks and Heartland Payment Systems: "The Visa and MasterCard regulations provide dispute-resolution and compensation rules when data breaches result in losses to issuers. The contractual obligations and compensation system, not tort law, are the Financial Institution Plaintiffs' only means of seeking compensation for economic losses."[145] The court recognized that while Heartland Payment System regularly exchanges information with issuer banks, they were not contracting parties.[146] The court saw no reason to insist on direct contractual privity between the parties given that there was a chain of privity through which redress could otherwise be sought.[147] With respect to the latter, the court emphasized the nature of the "comprehensive risk-allocation arrangement like the contracts and network requirements in this case."[148]

On appeal in *Lone Star*, the Fifth Circuit Court of Appeals questioned the district court's choice of the contracting parties paradigm.[149] The court was not convinced that the third-party scenario fit the conventional contracting parties mold. The court recognized that issuer and acquirer banks were linked via their mutual membership in the Visa and MasterCard networks; Heartland, the payment card processor, did not appear to be a member of those networks (although still bound by the terms of Visa and MasterCard networks via its con-

---

9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

Id. at 9. For further discussion of the PCI-DSS, see Sutherland Asbill & Brenna LLP, *Legal Alert: PCI DSS – What It Is and Why It Is Relevant to Your Business*, Lexology (Feb. 4, 2016), http://www.lexology.com/library/detail.aspx?g=94f604cc-acac-4d26-ac74-b9e329db1067; Robert J. Pile & Kristin Ward Cleare, *Pros and Cons of the Payment Card Data Security Standard*, Law360 (Mar. 1, 2016, 12:12 PM), http://www.law360.com/articles/765601/pros-and-cons-of-the-payment-card-data-security-standard ("[M]erchants typically are contractually obligated to comply with the PCI DSS.").

145. *In re Heartland*, 2011 WL 1232352, at *23–24.

146. *Id*. at *24.

147. *Id*.

148. *In re Heartland Payment Sys.*, 834 F. Supp. 2d at 590.

149. Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 423 (5th Cir. 2013).

tract with the acquiring bank), calling into question whether Heartland could access the dispute resolution mechanisms offered by Visa and MasterCard per their membership terms.[150] The court's main concern was that "[t]his uncertainty in the record leaves open the issue of Issuer Banks' bargaining power with respect to Heartland's participation in the Visa and Mastercard networks."[151] Specifically, according to the court, "[I]t is not clear that the allocation of risk 'could have been the subject of . . . negotiations' between Issuer Banks and Heartland by way of contracts with Visa and Mastercard."[152] The court does not even mention the PCI-DSS industry standards, which were central to the district court's contrary decision.

The Fifth Circuit Court of Appeals thus deployed the *People Express* stranger paradigm, permitting recovery for economic losses "where the defendant causes an identifiable class of plaintiffs to which it owes a duty of care to suffer economic loss that does not result in boundless liability."[153] Under the *People Express* standard, the issuing bank plaintiffs could be considered "particularly foreseeable" plaintiffs and "notions of fairness, common sense and morality" demanded that Lone Star be able to seek recovery for Heartland's alleged negligence.[154]

---

150. *Id*. at 426 ("[I]t is not clear whether Heartland's contracts with Acquirer Banks, which require Heartland to comply with Visa and Mastercard rules and regulations, provide the Issuer Banks with compensation mechanisms for losses that may be caused by [plaintiffs'] negligence.").

151. *Id*.

152. *Id*. (alteration in original) (quoting Travelers Indem. Co. v. Dannmann & Co., 594 F.3d 238, 248 (2010)).

153. *Id*. at 424.

154. *Id*. (quoting People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 116 (N.J. 1985)). That said, the court seemed to signal that if, after further development of the record, contractual remedies surfaced, recovery in tort would be unavailable. It was simply too early to dismiss a negligence claim without further development as to the nature of the relationship between the parties and what remedies would be afforded through these relationships.

Plaintiffs have subsequently relied on *Lone Star*'s foreseeability analysis to support merchant liability. *See, e.g*., Fin. Inst. and Consumer Plaintiffs' Joint Memorandum in Opposition to Target Corp.'s Motion to Stay Discovery at 9, *In re* Target Corp. Customer Data Sec. Breach Litig., No. 14-2522 (PAM/JJK), 2014 WL 10520603 (D. Minn. July 18, 2014) (noting that *Lone Star*'s "foreseeability" analysis recognized that Heartland could have foreseen that the issuing bank plaintiffs would be harmed as a result of Heartland's negligence). *But see* Reply Brief for Appellant Citizens Bank of Pa. at 5, Citizens Bank of Pa. v. Reimbursement Techs, Inc., No 14-3320, 2015 WL 636571, at *5 (3d Cir. Feb. 6, 2015) (arguing that the district court's ruling was in effect "an argument on the merits that was inappropriate at the Rule 12(b)(6) motion to dismiss stage") (quoting Indep. Enters. Inc. v. Pittsburgh Water & Sewer Auth., 103 F.3d 1165, 1176 n.9 (3d Cir. 1997)); Defendant's Reply to Plaintiffs' Opposition to the Motion to Dismiss the Consol. Class Action Complaint at 8, *In re* Target Corp. Customer Data Sec. Breach Litig., No. 14-2522 (PAM/JJK), 2014 WL 7014856 (D. Minn. Oct. 22, 2014) (characterizing *Lone Star* as merely holding that "New Jersey's economic loss doctrine could not be found applicable at the motion to dismiss stage").

The juxtaposition of *Heartland* and *Lone Star* provides a powerful example of the outcome-determinative nature of a court's choice of competing paradigms (i.e., stranger versus contracting parties) to address data breach claims. This is not the only such example, although it is particularly compelling given the different outcomes at trial and on appeal, with the different outcomes following from different choices of paradigm applied.

B. Stranger Paradigm Misapplied By Courts

Courts have misapplied the stranger paradigm in lieu of the contracting parties paradigm in a confusing manner. Moreover, the courts' starting place matters. Namely, courts are often led astray when they begin with consideration of the "special relationship" between the parties or an "independent tort duty" that arises between them, as opposed to considering first the contractual (or quasi-contractual) undertakings between the parties.

The seminal California case, *J'Aire Corp. v. Gregory*[155]—which has wielded influence in California and other jurisdictions—vividly illustrates the perils of disregard of the contracting parties paradigm in the context of the economic loss rule. In *J'Aire*, the California Supreme Court allowed J'Aire Corp., a restaurant owner, to recover purely financial losses from Gregory, a general contractor, whose negligence caused delay in the completion of a construction project at the premises where J'Aire Corp. leased space.[156] The landlord of the premises had a contract with Gregory for improvements on the premises and did not specify a date for completion of the work.[157] J'Aire Corp. alleged that the work was not completed within a reasonable time despite having no such guarantee in its lease from the landlord,[158] and that, as a result of the contractor's delay, it suffered business losses as a result of not being able to operate due to a lack of heat and air conditioning.[159]

Almost oblivious to the web of contractual relations between the parties, the court articulated what have come to be known as the "*J'Aire* factors" for determining whether parties owe one another a tort duty of care:

> (1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the de-

155. 598 P.2d 60 (Cal. 1979).
156. *Id*. at 62, 64.
157. *Id*. at 62.
158. *Id*.
159. *Id*.

> gree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct and (6) the policy of preventing future harm.[160]

California courts have applied these *J'Aire* factors to parties in privity of contract: "The cases, beginning with *J'Aire*, are clear and consistent in permitting recovery even when the economic injury is the only injury alleged; nor is the absence of a contract remedy a requisite."[161] California courts, in other words, apply *J'Aire* in all scenarios; it is this refusal to consider separately the stranger versus contracting parties paradigm that leads to confusion.

In *Music Group Macao Commercial Offshore Ltd. v. Foote*,[162] a case involving contracting parties, a California federal district court relied on *J'Aire*, and utilized the stranger paradigm in a confusing manner. In that case, a Philippines-based company contracted with the defendant, the company's former Chief Technology Officer (CTO), to provide information technology (IT) services.[163] The company subsequently suffered a cyberattack on its data systems rendering them unusable for one month and destroying much of the data contained within.[164] The plaintiff sued the defendant, asserting that in his role as CTO, he "breached his duty of care to Plaintiff and was grossly negligent when he failed to perform his obligations under the defined services of the Agreement."[165]

The court noted that California law recognized limited circumstances in which a party could maintain a tort action following a breach of contract.[166] The court held that, under the *J'Aire* factors,[167] no special relationship existed between the parties. The court likewise dispensed with the argument that the alleged fiduciary duty that the

160. *Id*. at 63. Gary Schwartz likewise criticized *J'Aire* as "ill-advised" in its attempt to define tort liability comprehensively. Schwartz argued that the decision posed a risk of overriding limitations on liability and disturbing obligations voluntarily assumed by contract. *See* Gary T. Schwartz, *Economic Loss in American Tort Law: The Examples of* J'Aire *and of Products Liability*, 23 SAN DIEGO L. REV. 37, 39–40 (1986).

161. Ott v. Alfa-Laval Agri, Inc., 37 Cal. Rptr. 2d 790, 800 (Ct. App. 1995).

162. No. 14-cv-03078-JSC, 2015 WL 3882448 (N.D. Cal. June 23, 2015).

163. *Id*. at *1.

164. *Id*. at *4.

165. *Id*. at *15.

166. According to the court, such circumstances include: "(1) when a product defect causes damage to other property; (2) when a defendant breaches a legal duty independent of the contract and (3) if a 'special relationship' existed between the parties." *Id*. Though the court did not explicitly note that the economic loss doctrine was implicated, it did conclude that only the latter two exceptions were implicated by the case, thereby implying that plaintiff's failure to sufficiently plead either of those exceptions would bar the negligence claim. *Id*.

167. J'Aire Corp. v. Gregory, 598 P.2d 60, 63–64 (Cal. 1979); *see supra* text accompanying note 160.

defendant owed created an independent duty running to the plaintiff.[168] The court did, however, find that a genuine issue of material fact existed as to whether a CTO provides "professional services" that create an extra-contractual "professional duty to use such skill, prudence and diligence as other members of the profession commonly possess and exercise."[169] Though the court could not find any cases where professional negligence principles had been extended to a CTO or other IT professional, it nonetheless held that a reasonable jury could conclude that a CTO, in his professional role, was responsible for network security.[170] The court also noted, "there is enough evidence before the Court from which a reasonable jury could find that other members of the corporate IT security profession would have taken certain steps to better protect Music Group from a cyber attack . . . ."[171] Accordingly, the court permitted the negligence claim to proceed on a professional services theory.

The *J'Aire* approach has led courts to disavow the contracting parties paradigm and has led to anomalous decisions in the data breach context. Consider, for example, the California federal district court's decision in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*,[172] a case involving the theft of user information stored by Sony in its PlayStation Network and Qriocity services.[173] As part of the user registration process for those services, users were required to enter certain personal information and agree to both Sony's Term of Service and Privacy Policy.[174] When Sony's data systems were breached, millions of users' data were stolen.[175] After discovery of the theft, Sony took its network services offline for over a month in order to audit its systems to discover the source of the breach, thereby

168. *See Music Group*, 2015 WL 3882448, at *15–16. The court deployed an interesting variant of a cheapest cost avoider argument: "[P]revention of future harm might be effected just as well without a finding of special relationship, as the onus would be placed on companies, not on their hires, to monitor tasks." *Id*. at *16.

169. *Id*. at *17; *see* Loube v. Loube, 64 Cal. Rptr. 2d 906, 911 (Ct. App. 1998) ("[U]nlike ordinary negligence, professional negligence breaches a duty that exists only because the parties have a contractual agreement, and it has been recognized that an action for professional negligence constitutes both a tort and a breach of contract.") (citing Neel v. Magana, Olney, Levy, Cathcart & Gelfand, 491 P.2d 421, 422–23 (Cal. 1971)).

170. *Music Group*, 2015 WL 3882448, at *17.

171. *Id.* ("It may be that there is no particular standard of care for Chief Technology Officers or IT consultants with respect to cyber security. . . . [But] Plaintiff's evidence creates a triable issue as to whether an individual in Defendant's position owes an independent tort duty based on the provision of professional services.").

172. 996 F. Supp. 2d 942 (S.D. Cal. 2014).

173. *Id*. at 954–55.

174. *Id*.

175. *Id*. at 955.

depriving the users of those online services from accessing certain functions through their PlayStation consoles and devices during that time.[176] Plaintiffs filed a class action lawsuit alleging negligence in Sony's failure to adequately protect plaintiffs' user information; and negligent misrepresentation for Sony's failure to timely disclose that the reason for the network downtime was a security breach.[177] Plaintiffs alleged injuries on account of "(1) expenses incurred to purchase credit monitoring services . . . (2) loss of use and value of Sony Online Services . . . (3) loss of use and value of Third Party Services . . . and (4) a diminution in value of Plaintiffs' Consoles."[178]

Sony urged the court to embrace the contractual parties paradigm and dismiss the claims. Sony insisted that "Plaintiffs' California negligence claim is nothing more than an attempt to plead around their contract with Sony, which clearly disclaims the economic losses Plaintiffs now seek to recover."[179] The court rejected Sony's framing of the case: "courts will generally enforce the breach of contractual promise through contract law, except when the actions that constitute the breach violate a *social policy* that merits the imposition of tort remedies."[180]

The court thus implicitly adopted the stranger paradigm and deployed the *J'Aire* factors as a universal test for duty. The court reasoned that "a plaintiff may be able to pursue both contract and tort remedies if the plaintiff alleges that the contractual breach also violated 'a *duty independent of the contract* arising from principles of tort law.'"[181] The court held that Sony owed an independent tort duty, namely the "duty to provide reasonable network security."[182] According to the court, such a duty was "well supported by both common sense and [state] law."[183] Moreover, the duty to provide network security "was separate and independent from the PSN User Agree-

176. *Id*.

177. *Id*. at 959.

178. *In re Sony Gaming Networks*, 996 F. Supp. 2d at 966.

179. *Id*. at 967–68.

180. *Id*. at 968 (emphasis added) (quoting Freeman & Mills, Inc. v. Belcher Oil Co., 900 P.2d 669 (Cal. 1995)). The court did acknowledge that "the economic loss doctrine was created to prevent 'the law of contract and the law of tort from dissolving one into the other.'" *Id*. (quoting Robinson Helicopter Co. v. Dana Corp., 102 P.3d 268, 273 (Cal. 2004)). Thus, "[a] person may not ordinarily recover in tort for the breach of duties that merely restate contractual obligations." *Id*. at 967–68 (quoting Aas v. Superior Court, 12 P. 3d 1125, 1135 (Cal 2004)).

181. *Id*. at 968 (emphasis added) (quoting *Aas*, 12 P.3d at 1136).

182. *Id*. at 966.

183. *Id*.

ment" and allowed plaintiffs to pursue both tort and contract remedies.[184]

Having determined that there was in fact an independent tort duty, the court nonetheless held that "negligence is the wrong legal theory on which to pursue recovery for Plaintiffs' economic losses" on account of plaintiffs' "fail[ure] to allege a 'special relationship' with Sony beyond those envisioned in everyday consumer transactions."[185] The court seems either to have confused the paradigms, or else to have embraced *sub rosa* the contracting parties paradigm, without admitting as much. It makes little sense for a court to embrace the stranger paradigm and determine that there is in fact an independent tort duty but then bar recovery on account of no "special relationship."

Moreover, the "independent duty" exception to the economic loss rule referred to in *Sony* is too broad and untethered from a close analysis of the extent to which the contracting framework provides a superior risk allocation mechanism (as even the *Sony* court seems to have concluded). The *Target* class action brought on behalf of financial institutions (as a companion case to the consumer class action considered above) provides another illustration of this phenomenon.[186] The Minnesota federal district court used the stranger paradigm to analyze whether Target was negligent with respect to the financial institutions that had to issue new cards as a result of the data breach.[187] The primary question was whether Target owed the banks a duty of care.[188] The court found a duty owed by the retailer to the financial institutions, relying heavily on Minnesota's Plastic Card Security Act, which requires businesses to meet certain security standards.[189] The court explained: "While courts are reluctant to recognize duties of care in the absence of legislative imprimatur, the duty to safeguard credit- and debit-card data in Minnesota has received that legislative en-

184. *In re Sony Gaming Networks*, 966 F. Supp. 2d at 968.

185. *Id*. at 969.

186. *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1309 (D. Minn. 2014).

187. The court analyzed the existence of a tort duty under Minnesota law, with no mention of the economic loss rule. *Id*. Defendants did not raise the economic loss rule as a defense. The court presumably deployed the stranger paradigm given that Minnesota (by statute) does not recognize the economic loss rule outside the products liability context.

188. Plaintiffs also asserted claims for negligence per se and a statutory cause of action under the Plastic Card Security Act, both of which survived the motion to dismiss. *Id*. at 1312–14.

189. *Id*. at 1310 (citing MINN. STAT. § 325E.64, subd. 3 (2007)). The Plastic Card Security Act forbids any entity conducting business in Minnesota from retaining security data for more than 48 hours after authorization of the transaction. *Id*. at 1312. For further discussion of this statute, see *infra* note 217.

dorsement."[190] The court did not grapple with the contrasting contracting parties paradigm—whereby the existence of a private network among banks and issuers weighs against the imposition of tort liability. To the contrary, the court noted that the voluntary assumption of duties indicated that the burden of liability was not too great for Target to bear.[191]

Finally, another recent data breach case, *In re Home Depot, Inc. Customer Data Security Breach Litigation*,[192] provides yet another vivid illustration of a court's analysis under the stranger paradigm, highlighting the capacious duty inquiry and giving short shrift to the nature of the contractual undertakings amongst the parties.[193] As with other payment card data breach cases, hackers broke into Home Depot's retail systems and accessed the personal information of "approximately 56 million Home Depot customers."[194] Financial institutions that had issued the payment cards used by Home Depot customers affected by the data breach brought a class action lawsuit.[195] The Georgia federal district court rejected Home Depot's motion to dismiss plaintiffs' negligence claim by giving wide berth to the "independent duty" exception to the economic loss rule. In so framing the case, the court gave little heed to the contracting parties paradigm.[196]

The court set the stage: "Here, even though there is a contract between the card issuers and the Plaintiffs, the independent duty exception would bar application of the economic loss rule."[197] The court then articulated a very expansive notion of duty—especially in the

190. *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d at 1310 ("[T]he legislature specifically acknowledged the availability of other causes of action arising out of a Minnesota company's failure to safeguard customers' information, stating that the remedies under the PCSA 'are cumulative and do not restrict any other right or remedy otherwise available' to the issuer banks.").

191. *Id*.

192. No. 14-md-2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016).

193. *Id*.

194. *Id*. at *1. The court emphasized in great detail that Home Depot was well aware of the weaknesses in its data retention systems and policies. *Id*. at *1–2. Specifically, the court made note of the numerous times across a five-year period leading up to the data breach that Home Depot was allegedly notified of its deficiencies by employees, third parties, and federal agencies, and nonetheless failed to adequately address them. *See id*. at *1–2.

195. *Id*. at *2.

196. *Id*. at *3–4.

197. *Id*. at *3. The terms of the contractual relationship are not clear. The court does not address whether the parties were in direct privity, or whether this was a similar "web of contracts" scenario as seen in other financial institution data breach claims. Nor does the financial institutions' complaint, which describes the payment card ecosystem in some detail, provide the answer. *See* Fin. Inst. Plaintiffs' Consol. Class Action Complaint at ¶¶ 84–88, *In re Home Depot*, 2015 WL 3814441.

context of pure financial losses—proclaiming that "Georgia recognizes a general duty 'to all the world not to subject them to an unreasonable risk of harm.'"[198] Given that Home Depot "caused foreseeable harm to a plaintiff," the court concluded that it "therefore owed a duty in tort."[199] Such an "independent duty" thereby "barr[ed] application of the economic loss rule."[200]

It is telling that the court cites the *In re Target* financial institutions class action in support of its tort duty holding. *In re Target* applies Minnesota law, which refuses to recognize the economic loss rule outside of the products liability context. Georgia, however, does recognize the contractual privity economic loss rule, albeit with an expansive "independent duty" exception. The court's analysis shows how the exception can swallow the rule; indeed, the court's analysis is seemingly unaffected by the existence of contractual relationships among the relevant parties. In this regard, the *Home Depot* court's tacit embrace of the stranger paradigm draws a marked contrast with similar cases deploying the contracting parties paradigm.

Consider *Silverpop Systems Inc. v. Leading Market Technologies*,[201] a breach-of-personal-information case that likewise applied Georgia law but accorded dispositive weight to the nature of the contractual relationship. Silverpop and Leading Market entered into a contract through which Silverpop granted use of an email marketing tool to Leading Market.[202] This tool retained a list of email addresses and other information that could then be accessed for the purpose of distributing marketing communications to customers.[203] In 2010, Silverpop's systems were illicitly accessed by an unauthorized party, who was able to obtain the stored email information of a number of Silverpop's customers, including Leading Market.[204]

---

198. *In re Home Depot*, 2016 WL 2897520, at *3 (quoting Bradley Ctr., Inc. v. Wessner, 296 S.E.2d 693, 695 (Ga. 1982)).

199. *Id*. ("Defendant knew about a substantial data security risk dating back to 2008 but failed to implement reasonable security measures to combat it.").

200. *Id*.

201. 641 F. App'x 849 (11th Cir. 2016) (per curiam), *aff'g in relevant part*, No. 12-cv-2513-SCJ, 2014 WL 11164763 (N.D. Ga. Feb. 18, 2014).

202. *Id*. at 850.

203. *Id*.

204. *Id*. Though Leading Market was informed of the breach, it continued to use Silverpop's services without making payment. After Silverpop suspended Leading Market's access to its services, Leading Market asserted that it was "operating under an understanding with Silverpop that the question of payment would be resolved after the parties came to an agreement on whether to renew the contract when it came ripe for renewal." *Id*. Silverpop then initiated an action in the Northern District of Georgia, seeking a declaratory judgment that Leading Market was not injured by the data breach, and thus Silverpop was not liable to Leading Market on, among other claims, a negligence theory. *Id*. at 850–51.

In deciding whether Leading Market's negligence claim was barred by the economic loss rule, the *Silverpop* court (like the *Home Depot* court) applied the Georgia contractual economic loss rule with the independent duty exception, but in *Silverpop*, the court's framing of the rule is remarkably different. The court began by reciting that Georgia's economic loss rule allows for recovery of damages to "property that is not the subject of [a] contract . . . on the premise that 'the duty breached in such situations generally arises independent of the contract.'"[205] The court concluded, however, that any duty to protect the email list at issue arose under the terms of the contract between the parties, which had included provisions within their contract governing the protection of confidential information.[206]

Silverpop and *Home Depot* thus exemplify divergent approaches to the application of the "independent duty" exception to the economic loss rule to data breach cases. In *Silverpop*, the existence of a well-defined contractual relationship between the parties led the court to channel the claims towards the terms of their contract.[207] In contrast, the *Home Depot* court found a "stranger" paradigm-type "general duty" owed to all to avoid inflicting harm on others.[208]

C. Contracting Parties Paradigm Reassessed

Given this evidence that courts have been misapplying the stranger paradigm in data breach cases, it is worth considering both why and what alternative is available to them. Here, the answer is related—courts are rejecting the contracting parties paradigm, at least as tradi-

---

205. *Id*. at 853 (quoting Bates & Assocs. v. Romei, 426 S.E.2d 919, 921 (Ga. Ct. App. 1993)).

206. *Id*. The court also rejected Leading Market's alternative arguments, that Georgia's "accident" and "misrepresentation" exceptions permit a negligence claim. *Id*. at 853–54. Under the accident exception, Georgia permits recovery of economic losses "for damages to [a] defective product itself, where the injury resulted from an accident." *Id*. at 854 (quoting Flintkote Co. v. Dravo Corp., 678 F.2d 942, 948 (11th Cir. 1982)). However, in order to justify application of the exception, the accident must constitute "a calamity, sudden violence, collision with another object, or some catastrophic event." *Id.* (quoting Busbee v. Chrysler Corp., 524 S.E.2d 539, 542 (Ga. Ct. App. 1999)). Noting that the parties entered into an agreement for a service, not a product, the court found that there was "no basis" for applying the "accident" exception to the negligence claim at issue. *Id*.

The court similarly found no basis to recognize a "misrepresentation" exception in the case. *Id*. Though Georgia recognizes such an exception, the court concluded that Leading Market failed to plead any claim of fraud or misrepresentation, either as separate counts or as part of its negligence pleading, to serve as a sufficient basis to apply the exception. *Id*. Instead, Leading Market's "sole . . . basis for the negligence claim is Silverpop's failure to protect against the data breach." *Id*.

207. *Silverpop*, 641 F. App'x at 853.

208. *In re* Home Depot, Inc. Customer Data Sec. Breach Litig., No. 14-md-2583-TWT, 2016 WL 2897520, at *3–4 (N.D. Ga. May 18, 2016).

tionally understood. This Section argues that the courts in *Lone Star*, *Music Group*, *Sony*, *Target*, and *Home Depot* should have analyzed the respective cases before them via the lens of the contracting parties paradigm, which would have affected the starting point—not necessarily the ending point—of each decision. This Article does not advocate for rigid application of the contractual privity economic loss rule consistent with a resolute preference for private ordering. Instead, after embracing the contracting parties paradigm as the starting point, courts should consider whether there are, nonetheless, powerful justifications for the imposition of tort liability.

1. The Contractual Liability Default

The contracting parties paradigm is a defensible starting point for courts' analyses. As a general matter, contracting parties internalize the costs and benefits of risks and outcomes within their transactions. As succinctly stated by the *Annett* court, it is often the case that parties who "contracted to assume certain risks of financial loss [also] had the ability to minimize these risks."[209] In other words, contracting parties can allocate risks and responsibilities amongst themselves efficiently so as to place responsibilities on the "cheapest cost avoiders."

Courts have an interest in encouraging such private ordering amongst contracting parties. In the data breach context, sophisticated parties, such as financial institutions and mega-retailers, are best equipped to identify and guard against such data breach risks—including via negotiation with the web of contracting parties—and it thus flouts reality to treat these actors as "strangers" to one another, even if they are not in direct privity of contract.

Courts' embrace of the contracting parties paradigm, as applied to the web of contracting parties in the data breach scenarios, would also encourage parties to devise and extend systems of industry regulation along the lines of the PCI-DSS standards, which were heavily relied on in *Heartland*. Five international payment card brands—American Express, Visa, MasterCard, Discover, and JCB—worked together to release the PCI-DSS in December, 2004.[210] Prior to the creation of PCI-DSS, each card brand followed its own standards in contractual relationships with entities within its network. The creation of such industry standards is likely to outperform regulation by tort liability,

209. Annett Holdings v. Kum & Go, L.C., 801 N.W.2d 499, 505 (Iowa 2011); *see supra* note 121 and accompanying text.

210. *See* Edward A. Morse & Vasant Raval, *Private Ordering in Light of the Law: Achieving Consumer Protection Through Payment Card Security Measures*, 10 DEPAUL BUS. & COM. L.J. 213, 229 (2012).

at least in terms of its ability to harness information and expertise by the industry actors. Individuals (especially consumers, but even financial institutions outside of the industry network) would then be able to argue that the actors fell short of these industry standards. Finally, it is likely that the emergence and development of a robust cyber risk insurance market would alter these networks of relationships and nudge parties to form stronger contractual ties.[211]

2. The Case for Tort Liability

The courts might still conclude that tort liability is warranted, but only once the plaintiff has made the case that, notwithstanding the voluntary allocation of risks and responsibilities between the contracting parties (or the potential for such allocation amongst a web of contracting parties) tort liability should be imposed by law. The strongest argument for imposition of such tort liability is the existence of externalized risks onto third parties, who are in essence strangers to the contracting parties paradigm. Tort is thus a stand-in for public regulation of the contracting parties.

Courts, in other words, should start with the contracting parties paradigm and then proceed to explore its limitations, if any, in the particular case. In *Sony*, for example, the court could have considered whether the application of a contractual privity economic loss rule would have left unremedied specific harms to third parties or more general societal externalities. Indeed, the court seems to have suggested as much when it referred to "actions that . . . violate a *social policy*" warranting a tort remedy.[212] The point here is not that the court's choice of paradigm would in fact be outcome determinative; the goal is for courts to apply a consistent and coherent framework that does not neglect the role for private ordering via contract.

---

211. Cybersecurity insurance is not yet widely adopted. *See, e.g.*, 2012 WORKING GROUP, *supra* note 11, at 13 (estimating 25% of companies have cybersecurity insurance policies); PONEMON INST., MANAGING CYBER SECURITY AS A BUSINESS RISK: CYBER INSURANCE IN THE DIGITAL AGE 4 (2013), http://www.ponemon.org/local/upload/file/Cyber%20Insurance%20white%20paper%20FINAL%207.pdf (estimating that 31% of companies have existing policies, whereas 57% claim they plan to purchase cybersecurity insurance in the future).

A recent RAND study—the first of its kind to collect and analyze over one hundred cyber insurance policies—noted that "PCI as an industry standard for payment processing was prominent in many questionnaires [issued by insurance carriers to assess security risks of applicants]." Sasha Romanosky et al., Content Analysis of Cyber Insurance Policies: How Do Carriers Develop Policies and Price Cyber Risk? 20 (Mar. 7, 2017) (unpublished manuscript) (on file with *DePaul Law Review*).

212. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 968 (S.D. Cal. 2014) (emphasis added).

Consider, in this vein, how the court in *Home Depot* implicitly concluded that imposing tort liability on the retailer placed liability on the cheapest cost avoider. The court reasoned that failing to place the burden of more stringent data security practices on Home Depot would allow virtually all companies that deal in sensitive information to avoid liability for their relaxed data security practices.[213] Thus, to justify the policy implications of its decision to find an expansive "legal duty to safeguard information" (notwithstanding any contractual undertakings between the parties), the court stated:

> To hold that no such duty existed would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyber attacks, leaving consumers with no recourse to recover damages even though the retailer was in a superior position to safeguard the public from such a risk.[214]

But how does the court know that the retailer is in the "superior position to safeguard the public"? The court's approach—starting with the stranger paradigm and then invoking a very expansive notion of duty, separate and apart from any contractual undertakings—leaves much to be desired. The better approach would be for the court to begin with a close examination of the allocation of risks and responsibilities among the parties operating within the credit card processing ecosystem.

Starting from the contracting parties paradigm would call for a more precise argument to be made by the plaintiff, and would undoubtedly raise the threshold for tort recovery. With a contractual liability default rule, the court would nonetheless entertain arguments that there are significant externalities not internalized within web of contracting parties. It is an empirical matter—based upon fine-grained analysis of industry conditions—whether third-party credit payment scenarios fit this description.[215] This judgment would not necessarily have to be made on a case-by-case basis in private litigation. The Washington State Legislature, for example, adopted a statute that governs negligence liability of credit card processors and vendors, making them liable to financial institutions for purely eco-

213. *In re Home Depot*, 2016 WL 2897520, at *3–4.

214. *Id*. at *4.

215. For a compelling argument that the consumer credit card network entails significant network externalities that justify the imposition of tort liability, see David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 939, 983 (2016). Opderbeck relies upon a growing economic literature. *See, e.g.*, Sujit Chakravorti, *Externalities in Payment Card Networks: Theory and Evidence* 1, 4–6, 31–32 (Fed. Reserve Bank of Chi. Pol'y Discussion Paper No. 2009-8, 2009); Hal Varian, *System Reliability and Free Riding*, *in* ECONOMICS OF INFORMATION SECURITY 1, 8–9 (L. Jean Camp & Stephen Lewis eds., 2004).

nomic losses if they fail to "take reasonable care to guard against unauthorized access to account information."[216]

Moreover, the "professionals" exception to the contractual privity rule can also fit this conceptual framework. Recall how the court in *Music Group* implicitly suggested the need to consider the "professionalization" of the IT services industry as a means to protect the wider public. Though the court was restrained from going as far as holding to that effect, it did seem open to the possibility that the same underlying rationale for recognizing extra-contractual duties for certain professionals (e.g., accountants, lawyers, architects, and environmental services professionals) may be applicable to IT professionals. The recognition of such a policy may go a long way towards opening up avenues for relief in data breach cases where plaintiffs would otherwise be barred by the economic loss rule. But, instead of operating as a blanket, categorical exclusion—with all of the attendant uncertainty regarding who qualifies as a "professional"—here, too, the burden should be on the plaintiff to demonstrate how, in the case of a contract with a particular professional, there are externalized third-party costs. Here, tort liability functions literally as regulation of contracting parties and should be justified, if at all, by consideration of the need for such regulation, especially in light of other public regulation of certain professionals.

V. Conclusion: The Regulatory Challenge of Data Breaches

The main goal of this Article is to frame the relevant questions courts should ask when faced with data security breach cases raising tort claims. It is appropriate for courts to begin—but not end—with the contracting parties paradigm, taking into account the mechanisms

216. Wash. Stat. Ann. § 19.255.020(3)(a) (West 2016). The provision reads:

> If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington as a consequence of the breach, even if the financial institution has not suffered a physical injury in connection with the breach.

Id. The statute also uses the PCI-DSS to provide "a 'safe harbor' by which entities would not be liable if they were 'certified compliant with the payment card industry data security standards adopted by the payment card industry security standards council, and in force at the time of the breach.'" Christopher Bosch, Note, *Securing the Smart Grid: Protecting National Security and Privacy Through Mandatory, Enforceable Interoperability Standards*, 41 Fordham Urb. L.J. 1349, 1405 n.305 (2014).

by which the parties voluntarily allocated risks and responsibilities between them (or could have taken advantage of existing institutional arrangements to do so). Courts should then consider whether, notwithstanding contractual (or quasi-contractual) relationships, there are significant externalities imposed on third parties. Drawing this altogether, courts should be in search of the cheapest cost avoider for imposition of liability; within this model, the existence of contract as the preferred method of allocation of risk and responsibility should be a significant factor, but one that could be outweighed in institutional contexts whereby such arrangements externalize significant risk onto hapless third parties.

Traces of such an analysis are buried within several of the data breach cases discussed so far. It does seem as if courts are motivated to address the negative externalities borne especially by consumers (but also including sophisticated players such as financial institutions) by imposing tort liability on merchants and other breached entities that the courts assume have the ability to minimize risks by adopting greater security measures. However, the courts are doing so not only in an ad hoc manner, but also by stretching and misapplying the stranger paradigm for the economic loss rule.

This Article advocates a broader regulatory perspective on the economic loss rule. To return full circle to where we began in the introduction, data breaches pose a regulatory challenge to which the federal and state governments, federal agencies, private industry, and private litigation have responded. We must therefore ask what is the optimal regulatory approach to address third-party externalities imposed by contracting parties? Consider the Washington Statute referenced above.[217] There, the legislature made a judgment to allow financial institutions to recover against credit card processors and vendors, regardless of contractual undertakings among the

217. Two additional state statutes incorporate PCI-DSS into data security statutes. Minnesota was "the first state to adopt legislation that effectively protects issuing banks from costs incurred to protect cardholders." Morse & Raval, *supra* note 210, at 246. The statute adopts some, but not all, of the requirements from the PCI-DSS. *See* James T. Graves, Note, *Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care*, 34 WM. MITCHELL L. REV. 1115, 1132 (2008) (discussing MINN. STAT. ANN. § 325E.64 (West 2007)). The Minnesota law establishes standards prohibiting the storage of personal data, and creates a cause of action for financial institutions to recover from entities that fail to meet the statute's requirements. *Id.* However, the law "only adopts a small subset of [PCI-DSS's] requirements." *Id.* at 1135. It is more permissive than the privately created standard, but does take steps to allow financial institutions to shift costs in the event of a breach. *Id.*

Nevada's law requires any data collector doing business in the state to comply with the current version of the PCI-DSS. *See* NEV. REV. STAT. ANN. § 603A.215 (2015). The statute does not expressly provide a cause of action or impose a penalty for noncompliance.

parties.[218] Cyberinsurance, moreover, can operate as a form of regulation by providing risk management services.[219] There is emerging evidence that suggests many firms rate themselves as under-prepared for a data breach and that insurance companies are working with firms to provide some (albeit at this point limited) support aimed at preventing breaches (as opposed to acting primarily to mitigate losses in the aftermath of a breach).[220]

To sum up, at present, tort liability (imposed as either exceptions to or end runs around the economic loss rule) would lead to a more robust cyberinsurance market, which predictably leads to further regulation—especially if there are third-party externalities. At that time, the economic loss rule can then forestall further tort liability. Seen in this broader regulatory perspective, the economic loss rule serves to police the boundary not only between tort and contract, but, even more so, between tort and regulation as alternative mechanisms to regulate contractual parties.

---

218. Such a policy judgment might be misguided. Richard Epstein and Thomas Brown have criticized Minnesota's statutory provision, on the ground that it does not account for "all of the other provisions of the elaborate contracts that currently bind participants in the payment card networks. In particular, the statute completely fails to recognize the fact that the shift in the liability rules may increase the costs of payment card acceptance to merchants to the point that they either drop out of the systems entirely or demand some reduction in the fees that they pay." Richard A. Epstein & Thomas P. Brown, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203, 222 (2008). My only point here is that such a policy judgment could be appropriate if based upon findings of third-party externalities, which would justify further regulation of the contractual parties.

219. 2012 WORKING GROUP, *supra* note 11, at 1 (describing cybersecurity insurance as an "'effective, market-driven way of increasing cybersecurity' because it may help reduce the number of successful cyber attacks by promoting widespread adoption of preventative measures"). More specifically, by offering lower premiums to firms that adopt specific safeguards, insurance can incentivize good cybersecurity practices. *Id.* at 5; *see also* Sales, *supra* note 8, at 1536 (discussing how insurance companies can provide "second-order regulation, enforcing cyber-security standards by refusing to bear the losses of firms with poor records or engaging in price discrimination against them").

220. *See* 2014 WORKING GROUP, *supra* note 11, at 3 (suggesting that increasing dialogue between insurance carriers and potential insureds will "harness the incentivizing effect of private insurance contracts to promote more informed and effective cybersecurity practice"). A recent high profile example is the partnership between Microsoft, which developed "Secure Score" to rate the security settings of commercial customers that use Office 365, and Hartford Financial Services Group Inc., the first company to announce publicly that it will use Microsoft's Secure Score as a factor in determining premiums for cyberinsurance. *See* Jay Greene, *Microsoft to Rate Corporate Cybersecurity: Hartford Financial Says It Will Use the Office 365 Secure Score When Setting Cyberinsurance Rates*, WALL ST. J. (Feb. 10, 2017), https://www.wsj.com/articles/microsoft-to-rate-corporate-cybersecurity-1486749600 ("It gives us insight and comfort that you are doing some risk management." (quoting Tom Kang, Hartford's head of cyberinsurance)). The recent RAND study provides further evidence that insurance companies are moving in this direction by furnishing detailed security questionnaires to applicants, asking a range of questions relating to "IT, management and policy/compliance practices adopted by the applicant." Romanosky et al., *supra* note 211, at 15.