Mainstreaming Unjust Enrichment and Restitution in Data Security Law

Ying Hu*

This Article seeks to improve enforcement of the duty of companies to safeguard personal data in their possession. It is notoriously difficult for data breach victims to succeed in class actions against companies that failed to take reasonable steps to safeguard their personal data. Many commentators have argued that existing legal rules should be relaxed or applied differently in data breach cases.

This Article argues instead that litigants and the courts should take more seriously unjust enrichment as a cause of action in those cases. The Article makes two main contributions. First, it critically analyzes the two main theories of unjust enrichment observed in data breach cases: the overpayment theory and the "would not have shopped" theory. It in turn proposes an alternative, and more plausible, account of the elements that must be proved for the overpayment theory. Second, it explains how the facilitative effects of these unjust enrichment claims on class actions solve a powerful enforcement deficit with respect to data security.

* Assistant Professor, National University of Singapore. J.S.D. & LL.M., Yale Law School; LL.M., University of Cambridge; LL.B., University of Hong Kong. Many thanks to Christine Jolls, Andrew Kull, Rory Gregson, Hans Tjio, James Penner, Jaclyn Neo, Kenneth Khoo, Kevin Tan, Justin Tan, Tan Zhong Xing, Tan Cheng Han, Sandra Booysen, Helena Whalen-Bridge, Kumaralingam Amirthalingam, Kelvin Low, Christian Witting, and Tan Hsien-Li for their invaluable comments and discussions. I would also like to thank Miranda Tafoya and fellow editors at the *UC Irvine Law Review* for their superb feedback and assistance during the editing process. All mistakes are mine.

INTRODUCTION

Data breach victims have to overcome multiple legal hurdles to seek relief against companies that failed to take reasonable steps to safeguard their personal data.[1] For the purposes of this Article, "data breach" refers to any unauthorized access, collection, disclosure, or use of personal data as a result of inadequate data security. So far, data breach victims have had very limited success. Courts have dismissed their tort claims for failure to establish that companies owed them a duty to protect their data[2] or a duty to protect them from pure economic loss,[3] that the duty was breached, that there was a legally cognizable loss,[4] or that their loss was causally linked to the breach.[5] Their contract claims have failed for similar reasons.[6] In particular, multiple courts have held that promises contained in privacy policies

---

1. For the purpose of this Article, "personal data" is used loosely to refer to not only information about individuals' personal attributes and characteristics, but also information about the activities that they carry out while using certain products or services.

2. *See, e.g.*, McConnell v. Dep't of Lab., 345 814 S.E.2d 790, 799 (Ga. Ct. App. 2018); Cooney v. Chi. Pub. Schs., 943 N.E.2d 23, 29 (Ill. App. Ct. 2010). Plaintiffs have also had mixed success in bringing negligence per se claims based on alleged violations of privacy and consumer protection statutes, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), and the Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45. *See, e.g.*, *In re* Blackbaud, Inc., 567 F. Supp. 3d 667, 683–84 (D.S.C. 2021) (HIPAA); *In re* Sonic Corp. Customer Data Sec. Breach Litig. (Fin. Inst.), No. 1:17-md-2807, MDL No. 2807, 2020 U.S. Dist. LEXIS 114891, *13–14 (N.D. Ohio July 1, 2020) (FTC Act). *See also infra* Part IV.

3. *See* Bernard Chao, *Privacy Losses as Wrongful Gains*, 106 IOWA L. REV. 555, 565–66 (2021).

4. Plaintiffs have sought to argue that that they have suffered loss because (a) they have been deprived of certain use value of their personal data or (b) their personal data has diminished in value as a result of data breaches. But these arguments have had limited success. *See, e.g.*, *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F. 3d 125, 149 (3d Cir. 2015) ("They allege no facts suggesting that they ever participated or intended to participate in [a market for internet history information], or that the defendants prevented them from capturing the full value of their internet usage information for themselves. For example, they do not allege that they sought to monetize information about their internet usage, nor that they ever stored their information with a future sale in mind. Moreover, the plaintiffs do not allege that they incurred costs, lost opportunities to sell, or lost the value of their data as a result of their data having been collected by others."). *C.f. In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-md-02752, 2017 U.S. Dist. LEXIS 140212, 65–66 (N.D. Cal. Aug. 30, 2017) (finding that the plaintiffs plausibly alleged injury in the form of diminution in value of personal data where such data was allegedly sold by hackers on the dark web). Courts have also refused to recognize lost time and effort, as well as non-medically diagnosable emotional distress, in and of itself as a cognizable injury. *See, e.g.*, *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 4 A.3d 492, 498 (Me. 2010) ("Maine law of negligence and implied contract does not recognize time and effort alone, spent in a reasonable effort to avoid or remediate reasonably foreseeable harm, as a cognizable injury in the absence of physical harm or economic loss or identity theft."); Baldwin v. Nat'l W. Life Ins. Co., No. 2:21-cv-04066, 2021 U.S. Dist. LEXIS 175229, at *11–12 (W.D. Mo. Sept. 15, 2021).

5. *See, e.g.*, Stollenwerk v. Tri-West Health Care All., 254 F. App'x 664, 668 (9th Cir. 2007) (noting that a mere "temporal connection[]" between the data breach and the plaintiffs' loss was not sufficient to establish causation).

6. *See, e.g.*, *In re Hannaford*, 4 A.3d at 497 ("[E]motional distress suffered as a result of breach of contract is ordinarily not recoverable unless it is accompanied by physical injury or it results in serious emotional disturbance due to the nature of the contract."); Svenson v. Google Inc., 65 F. Supp. 3d 717, 725 (N.D. Cal. 2014) (holding that an allegation that disclosure of contact information increased risk of identity theft was "too speculative" to satisfy the contract damages requirement); Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 917–18 (N.D. Cal. 2009) (holding that plaintiff could not present evidence of actual damage because he had not been an identity theft victim), *aff'd*, 380 F. App'x 689, 691 (9th Cir. 2010).

are not contractually binding.[7] Courts have also dismissed many claims based on violations of federal or state privacy and consumer protection laws because the plaintiffs could not show that they relied on the defendant's misconduct,[8] that they suffered pecuniary loss,[9] or that the statute provided a private cause of action.[10] Standing presents a particularly thorny problem. Federal appellate courts have taken different, and sometimes conflicting, approaches to deciding whether a data breach victim has satisfied the injury-in-fact requirement under Article III of the Constitution.[11] A number of courts appear reluctant to confer Article III standing on plaintiffs who have not yet suffered any data misuse, particularly if they fail to show that at least some victims of the same data breach have already experienced data misuse.[12] Finally, it is far from clear to what extent data breach victims can join a class action. Courts have denied class certification in putative data breach class actions on the basis that Rules 23(a) and 23(b) of the Federal Rules of Civil Procedure are not satisfied.[13]

Many commentators argue that existing legal rules should be relaxed or applied differently in data breach cases. Some advocate imposing additional duties on database holders.[14] Some suggest a more nuanced approach to the economic loss

---

7. One empirical study suggests that U.S. courts tend to treat privacy policies as contracts in the majority of cases. Oren Bar-Gill, Omri Ben-Shahar & Florencia Marotta-Wurgler, *Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts*, 84 U. CHI. L. REV. 7, 25–30 (2017). Other studies suggest otherwise. *See* Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REG. 45 (2019).

8. *See, e.g.*, *In re* Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 514, 542 (M.D. Pa. 2021).

9. Various federal and state laws require proof of "damage" or "loss." Plaintiffs have sought to argue that loss of personal data through unauthorized use or release of personal data amounts to a loss of money or property. However, the courts have often rejected such arguments. *See, e.g.*, *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F. 3d 125, 149 (3d Cir. 2015) (Computer Fraud and Abuse Act); Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1127 (CAL. BUS. & PROF. CODE § 17200); Jackson v. Loews Hotels, Inc., No. ed-cv-18-827, 2019 U.S. Dist. LEXIS 124525, at *14–15 (C.D. Cal. July 24, 2019) (California's Unfair Competition Law). The Supreme Court also held that uncorroborated allegations of emotional distress are inadequate to satisfy the actual damages requirement for the purpose of the Privacy Act of 1974. *See* Doe v. Chao, 540 U.S. 614, 617–18 (2004).

10. For example, some statutes, such as the FTC Act and HIPAA, do not provide a private cause of action.

11. Some courts have recognized that a plaintiff can establish Article III standing based on an increased risk of future injury. *See, e.g.*, McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295 (2d Cir. 2021); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010); Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017). Other courts seem reluctant to confer Article III standing on plaintiffs who have not yet suffered any data misuse. *See infra* note 12.

12. *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012); Whalen v. Michaels Stores, Inc., 689 Fed. App'x. 89 (2d Cir. 2017); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017); *In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 771–72 (8th Cir. 2017); Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332 (11th Cir. 2021).

13. *See infra* Part II.

14. *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016) (arguing that digital media companies that collect and use personal data should be classified as "information fiduciaries"); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 14 (2020) ("Information fiduciaries have three basic kinds of duties toward their end users: a duty of confidentiality, a duty of care, and a duty of loyalty. The duties of confidentiality and care require digital companies to keep their customers' data confidential and secure.") [hereinafter *The*

rule.[15] Others argue for recognizing more types of harm (in particular, psychological harms) as cognizable injuries.[16]

This Article takes a less trodden path. It suggests that litigants and the courts should take more seriously unjust enrichment as a cause of action in data breach cases. Briefly stated, an unjust enrichment claim asserts that (1) the defendant received payment (in the form of either money or personal data) from the plaintiff; and (2) it is inequitable for the defendant to retain that payment either because (a) the payment was intended to pay for adequate data security, which the defendant failed to provide (the "overpayment" theory), or because (b) the plaintiff would not have made payment had she known about the defendant's inadequate data security (the "would not have shopped" theory).[17] In both cases, the unjust enrichment claim relates to a financial benefit, rather than emotional distress;[18] the plaintiff seeks to restore a benefit that she previously conferred on the defendant, rather than seeking compensation for damage suffered following a data breach.[19] As a result, unjust enrichment does not require the plaintiff to overcome as many legal hurdles to establish a viable claim. More importantly, even if a data breach victim has not yet suffered any identity theft or fraud, she may be able not only to establish

Fiduciary Model of Privacy]; Adam Schwartz & Cindy Cohn, *"Information Fiduciaries" Must Protect Your Data Privacy*, ELEC. FRONTIER FOUND. (Oct. 25, 2018), https://www.eff.org/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy [https://perma.cc/D5GV-878D]; Meiring de Villiers, *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, 30 HASTINGS COMMC'NS & ENT. L.J. 419 (2008) (arguing that database owners should be liable for failing to patch certain computer security vulnerabilities where their failure foreseeably encourages "free radicals" to commit a tort or crime); Vincent R. Johnson, *Data Security and Tort Liability*, 11 J. INTERNET L. 22 (2008) (claiming that database possessors should owe a duty towards data subjects to mitigate reasonably perceivable risk of harm); Doug Lichtman & Eric A. Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 222–23 (2006) (arguing in favor of imposing a duty on internet service providers to prevent cyberattacks); Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140 (2006) (advocating for a new tort of information misuse based on the Fair Information Practice Principles). *Cf.* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135 (2019) (arguing that the law is already settling upon a well-defined duty of data security).

15. *See* Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?,* 66 DEPAUL L. REV. 339 (2017).

16. *See* Ido Kilovaty, *Psychological Data Breach Harms*, 23 N.C. J.L. & TECH. 1 (2021) (arguing for the recognition of psychological data breach harms); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018) (arguing that anxiety and risk should be recognized as compensable harms) [hereinafter *Risk and Anxiety*]; Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 364 (2014) (suggesting it might sometimes be appropriate to assume privacy harm upon proof of violation)*; see also* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms,* 102 B.U. L. REV. 793 (2022) (proposing to recognize more types of cognizable harm in privacy cases in general) [hereinafter *Privacy Harms*].

17. *See infra* Section I.A and Section I.B.

18. Plaintiffs who have only suffered non-medically diagnosable emotional distress are likely to experience difficulty establishing various types of claims. *See supra* notes 4 and 9.

19. As for the difficulties with recovering such consequential loss, see *supra* Introduction and notes 4–6 as well as *infra* Section II.B.

standing to bring an unjust enrichment claim,[20] but also, as analyzed in detail below, to participate in a class action.[21]

In recent years, an increasing number of unjust enrichment claims concerning data breach have survived motions to dismiss.[22] However, privacy scholars have largely overlooked these cases.[23] Notable exceptions are Bernard Chao, Lauren Scholz, and Lior Strahilevitz. Bernard Chao argues that disgorgement should be available as a remedy for breach of contractual obligations relating to privacy, including contractual obligations to secure personal data.[24] Lauren Scholz argues in favor of awarding restitutionary remedies against certain persons who acquire personal data without authorization.[25] By contrast, this Article considers unjust enrichment as a standalone cause of action against persons that failed to provide adequate data security, which remains underexplored in the existing literature.[26] Additionally, Lior Strahilevitz suggests that plaintiffs who succeed in establishing unjust enrichment claims in data breach cases should have little difficulty satisfying the injury-in-fact requirement under Article III of the Constitution.[27] The author agrees with Strahilevitz and further explains in Part II below how the unjust enrichment cause of action, in facilitating class actions, solves a significant enforcement deficit with respect to data security.

In Part I, this Article critically analyzes two theories of unjust enrichment claims that have emerged from existing data breach cases: the overpayment theory and the "would not have shopped" theory. It proposes a different and more plausible account of the elements that must be proved for the overpayment theory. It also clarifies the main elements of a claim based on the "would not have shopped" theory. The analysis in this Part has implications not only for data breach cases but also for other privacy claims. In recent years, plaintiffs have brought unjust enrichment claims to vindicate various types of privacy wrongs, including unauthorized collection, storage, and disclosure of personal data, as well as use of personal data for purposes unauthorized by data subjects.[28] Clarifying the elements of unjust enrichment claims in data breach cases provides guidance for litigants in those cases, who often seek relief based on essentially the same theories (i.e., overpayment and "would not have shopped").

---

20. Lior Jacob Strahilevitz, *Data Security's Unjust Enrichment Theory*, 87 U. CHI. L. REV. 2477, 2485–88 (2020).

21. There is likely less objection to allowing a class action based on the overpayment theory than the "would not have shopped" theory. *See infra* Section II.B.2.

22. *See infra* Section I.A and Section I.B.

23. Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 675 (2019) (claiming that judges and lawyers overlook restitution largely due to historical reasons). Chao, *supra* note 3, at 572 ("To date, most privacy scholars have overlooked restitution.").

24. Chao, *supra* note 3, at 574 ("This Article is focused on just one of restitution's remedies: disgorgement.").

25. *See generally* Scholz, *supra* note 23.

26. Chao does acknowledge unjust enrichment as a standalone cause of action. He does not, however, consider in any detail the elements of an unjust enrichment claim in data security cases. *See* Chao, *supra* note 3, at 591–95. Scholz suggests that individuals can bring unjust enrichment claims against a person who acquires their personal data through questionable means (as opposed to a person who fails to provide adequate data security). *See* Scholz, *supra* note 23, at 671–72.

27. Strahilevitz, *supra* note 20, at 2478–80.

28. *See infra* Section I.C.

Part II describes how the facilitative effects of unjust enrichment claims on class actions solve a powerful enforcement deficit with respect to data security. Data breach actions are often brought as class actions because the amount of injury suffered by individual data breach victims is not sufficiently large to incentivize them to bring individual lawsuits. This Article argues that the unjust enrichment claims discussed in this Article are more amenable to class-action resolution than claims that seek to recover loss from data misuse, mitigation costs, or emotional distress for two related reasons: (1) there is less divergence in interests between putative class members; and (2) it is easier to assess the remedy on a class-wide basis.[29]

Part III addresses the threat of contractual exemption clauses and other contract-related limits on unjust enrichment claims in response to data breaches. In particular, it examines the traditional rule that no unjust enrichment claims can be brought where the parties have a valid and existing contract governing the same subject matter, which many courts have relied on to dismiss unjust enrichment claims in data breach cases.[30] This Article recognizes an arguable case for disapplying this rule to unjust enrichment claims based on overpayment for data security.

Finally, Part IV considers various circumstances in which data breach victims might be able to seek restitution as a remedy for breach of common law or statutory duties to secure personal data.

I. UNJUST ENRICHMENT IN DATA BREACH CASES

In recent years, an increasing number of unjust enrichment claims concerning data breaches have survived motions to dismiss. The courts in those cases have recognized two theories of unjust enrichment: the overpayment theory and the "would not have shopped" theory. However, on a closer analysis, the courts have likely misstated the key elements of the overpayment theory. This Part in turn proposes an alternative, and arguably more appropriate, account of those elements. Moreover, this Part clarifies the elements of a claim based on the "would not have shopped" theory. Finally, this Part explains why the unjust enrichment cause of action is not rendered redundant by the availability of an action for breach of contract for defective data security.

A. The Overpayment Theory of Unjust Enrichment

This Section first demonstrates that data breach victims have had some, albeit limited, success in bringing unjust enrichment claims based on overpayment for data security. It then considers what data breach victims must prove to establish each of the three main elements of an unjust enrichment claim: (1) enrichment; (2) at the plaintiff's expense; and (3) circumstances which render it unjust for the defendant to retain the enrichment.[31] In particular, it argues that the approaches

29. *See infra* Part II.

30. *See infra* Section III.A.

31. Section 1 of the RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT (AM. L. INST. 2011) states, "[a] person who is unjustly enriched at the expense of another is subject to liability in restitution."

taken by the Eleventh and the Eighth Circuits to determine the existence and extent of enrichment are both unsatisfactory and proposes an alternative test. Finally, this Section highlights several benefits of adopting the overpayment theory of unjust enrichment as proposed in this Article.

1. Resnick and Kuhns

While data breach victims successfully pleaded an unjust enrichment claim based on overpayment for data security in *Resnick v. AvMed*,[32] they failed to do so in *Kuhns v. Scottrade*,[33] in which the court applied a stricter test for establishing enrichment.

In *Resnick*, two laptops stolen from AvMed's office contained sensitive customer information of approximately 1.2 million customers, which included protected health information, Social Security numbers, names, addresses, and phone numbers.[34] AvMed, a company providing health plans, did not secure those laptops. The plaintiffs brought a putative class action against AvMed for negligence, breach of contract, breach of fiduciary duty, and unjust enrichment.[35] The Eleventh Circuit held that the plaintiffs alleged sufficient facts for their unjust enrichment claim to survive a motion to dismiss.[36]

To establish an unjust enrichment claim under Florida law, a plaintiff must show that:

(1) the plaintiff has conferred a benefit on the defendant;

(2) the defendant has knowledge of the benefit;[37]

(3) the defendant has accepted or retained the benefit conferred; and

(4) the circumstances are such that it would be inequitable for the defendant to retain the benefit without paying fair value for it.[38]

According to the majority in *Resnick*, the plaintiffs successfully alleged all four elements.[39] They alleged that they conferred a benefit on AvMed in the form of monthly premiums and AvMed appreciated or knew of the benefit.[40] Moreover, it would be inequitable for AvMed to retain the premiums because AvMed used them to pay for the "administrative costs of data management and security" and failed to implement security measures that were "mandated by industry standards."[41]

Many district courts around the country have approved of overpayment for data security as a plausible basis for an unjust enrichment claim in data breach cases:

---

32. *Resnick*, 693 F.3d 1317 (11th Cir. 2012), *settled*, Curry v. AvMed, Inc., No. 10-cv-24513, 2014 U.S. Dist. LEXIS 48485 (S.D. Fla. Feb. 28, 2014).

33. *Kuhns*, 868 F.3d 711 (8th Cir. 2017).

34. *Resnick*, 693 F.3d at 1322.

35. *Id.* at 1321.

36. *Id.*

37. This element is sometimes criticized as superfluous. *See* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 cmt. d (AM. L. INST. 2011).

38. *Resnick*, 693 F.3d at 1328 (citing Della Ratta v. Della Ratta, 927 So. 2d 1055, 1059 (Fla. Dist. Ct. App. 2006)).

39. *Id.*

40. *Id.*

41. *Id.*

plaintiffs who paid the defendant for insurance policies,[42] healthcare services,[43] credit services,[44] and products,[45] have successfully alleged that it would be inequitable for the defendant to retain all that payment because the plaintiffs did not receive the benefit of securely maintained personal data (since their data was disclosed in one or more data breaches). As such, their unjust enrichment claims survived a motion to dismiss.

Nevertheless, other courts are more skeptical of the overpayment theory of unjust enrichment.[46] For example, the Eighth Circuit appeared to adopt a more stringent test for establishing an unjust enrichment claim based on overpayment for data security in *Kuhns v. Scottrade*.[47] In *Kuhns*, hackers accessed the internal database of Scottrade, a securities brokerage firm, and acquired the personal data of over 4.6 million Scottrade customers.[48] Affected by the data breach, Kuhns and three others brought a putative class action against Scottrade. Similar to the plaintiffs in *Resnick*, Kuhns argued that a portion of his brokerage service fees was "used for data management and security," and that Scottrade provided deficient cybersecurity, resulting in a data breach.[49] On that basis, he allegedly overpaid Scottrade for brokerage services. However, the Eighth Circuit dismissed Kuhns' unjust enrichment claim on several grounds, one of which is that he failed to allege that "any specific portion of [his brokerage services fees] went toward data protection."[50] In reaching this decision, the court relied on a similar Eighth Circuit decision, *Carlsen v. GameStop, Inc.*,[51] which dismissed an unjust enrichment claim based on overpayment of subscriber fees because the plaintiff did not "allege that any specific portion of his subscriber fee went toward data protection."[52] By

42. *See, e.g.*, Baldwin v. Nat'l W. Life Ins. Co., No. 21-cv-04066, 2021 U.S. Dist. LEXIS 175229 (W.D. Mo. Sept. 15, 2021); *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1201 (D. Or. 2016) ("Plaintiffs allege that they made payments to Premera and that under the circumstances it is unjust for Premera to retain the benefits received without payment. This is sufficient to withstand a motion to dismiss.").

43. *See, e.g.*, *In re* Eskenazi Health Data Incident Litig., No. 49D01-2111, Ind. Super. LEXIS 130 (Ind. Super. Ct. Sep 2, 2022); *In re* Ambry Genetics Data Breach Litig., 567 F. Supp. 3d 1130 (C.D. Cal. 2021); Wallace v. Health Quest Sys., No. 20-cv-545, 2021 U.S. Dist. LEXIS 54557 (S.D.N.Y. Mar. 23, 2021); Fox v. Iowa Health Sys., 399 F. Supp. 3d 780 (W.D. Wis. 2019); Lozada v. Advoc. Health & Hosps. Corp., No. 1-18-0320, 2018 Ill. App. Unpub. LEXIS 2394 (Ill. App. Ct. 2018); *In re* Banner Health Data Breach Litig., No. cv-16-02696, 2017 U.S. Dist. LEXIS 221534, at *19 (D. Ariz. Dec. 20, 2017) ("Plaintiffs allege that they paid money to Defendant for insurance plan premiums and healthcare service, that part of the money was supposed to be used for the administrative costs of data security, and that Defendant failed to provide adequate data security. These allegations are sufficient to support a claim for unjust enrichment.").

44. *See, e.g.*, *In re* Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 411–13 (E.D. Va. 2020).

45. *See, e.g.*, *In re* Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 514 (M.D. Pa. 2021); Rudolph v. Hudson's Bay Co., No. 18-cv-8472, 2019 U.S. Dist. LEXIS 77665 (S.D.N.Y. May 7, 2019); Bray v. GameStop Corp., No. 17-cv-1365, 2018 U.S. Dist. LEXIS 226220 (D. Del. Mar. 16, 2018).

46. The federal district courts have been inconsistent in adopting the overpayment theory. *See, e.g.*, *In re Rutter's*, 511 F. Supp. 3d at 538–39 (collecting conflicting decisions).

47. Kuhns v. Scottrade, 868 F.3d 711, 718 (8th Cir. 2017).

48. *Id.* at 713–14.

49. *Id.* at 715. *See* Resnick v. AvMed, 693 F.3d 1317, 1328 (11th Cir. 2012).

50. *Kuhns*, 868 F.3d at 718 (citing Carlsen v. GameStop, Inc., 833 F.3d 903, 912 (8th Cir. 2016)).

51. Carlsen v. GameStop, Inc., 833 F.3d 903, 912 (8th Cir. 2016).

52. *Id.*

contrast, the Eleventh Circuit did not find it necessary for the plaintiffs to show that any specific portion of their insurance premiums paid for data security in *Resnick*.[53]

2. Elements of an Unjust Enrichment Claim

Apart from Florida, many states recognize a cause of action for unjust enrichment.[54] The exact elements of the cause of action vary in different states.[55] Broadly speaking, to bring an unjust enrichment claim, a plaintiff must establish that the defendant has received a benefit from the plaintiff "under circumstances making it inequitable for the defendant to retain the benefit."[56] Each element is considered in turn. For the purpose of our discussion, the defendant is assumed to be a company that allegedly failed to take adequate data security measures.

a. Enrichment

A defendant is enriched if it receives benefits that lead to an increase in its wealth.[57] On a closer examination, neither the court in *Resnick* nor the court in *Kuhns* accurately stated what must be proved to establish an unjust enrichment claim based on overpayment for data security. This Section first explains why the approaches in both *Resnick* and *Kuhns* are unsatisfactory. It then proposes an alternative test for determining whether the defendant has been enriched in data breach cases.

i. Resnick and Kuhns Re-examined

To begin with, let us consider the enrichment in *Resnick*. If the enrichment was the entire "monthly premiums," as the court appeared to suggest,[58] then the plaintiffs could not maintain that the enrichment was unjust since AvMed already performed the most important part of its obligations under the insurance contract—providing insurance coverage. What the Eleventh Circuit most likely meant is that AvMed was enriched by the amount of payment which was intended

---

53. *Resnick*, 693 F.3d at 1328.

54. *See, e.g.*, *In re* Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 411 (E.D. Va. 2020) ("The substantive law of unjust enrichment is largely consistent across each of the relevant jurisdictions [i.e., California, Florida, New York, Texas, Virginia, Washington]."); Powers v. Lycoming Engines, 245 F.R.D. 226, 231 (E.D. Pa. 2007), *rev'd on other grounds*, 328 Fed. App'x 121 (3d Cir. 2009) ("Although there are numerous permutations of the elements of the cause of action in the various states, there are few real differences.").

55. *See, e.g.*, Vista Healthplan, Inc. v. Cephalon, Inc., No. 06-cv-1833, 2015 U.S. Dist. LEXIS 74846, at *81–84 (E.D. Pa. June 10, 2015) (explaining various ways that the unjust enrichment laws vary in different states, for example, some states, such as California, Florida, Kansas, Maine, Massachusetts, Nevada, New Mexico, North Carolina, South Dakota, Tennessee, Utah and Wisconsin, require proof that the defendant appreciates or knows of the benefit).

56. *See, e.g.*, RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 cmt. d (AM. L. INST. 2011); *In re Capital One*, 488 F. Supp. 3d at 411 ("Broadly stated, the elements of an unjust enrichment claim are the receipt of a benefit and the unjust retention of the benefit at the expense of another.").

57. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 cmt. d (AM. L. INST. 2011) (stating restitution is concerned with the receipt of benefits that yield a measurable increase in the recipient's wealth).

58. *Resnick*, 693 F.3d at 1328.

by the parties to pay for adequate data security. If that were the case, then the plaintiffs would have to provide sufficient facts to demonstrate that at least a portion of the monthly premiums was meant to pay for data security. In *Resnick*, the plaintiffs merely alleged that the defendant (a) had knowledge of monthly premiums paid by the plaintiffs; and (b) used those premiums to pay for data management and security.[59] These facts alone, however, are insufficient to establish the purpose for which the premiums were received. The mere fact that AvMed subsequently used the premiums for a particular purpose cannot by itself show that AvMed received premiums for that purpose. For example, AvMed may have used the premiums to pay salaries to its employees—this by no means suggests that the plaintiffs could bring an unjust enrichment claim against AvMed if AvMed failed to pay its employees. In short, the unjust enrichment claim in *Resnick* arguably should have been dismissed because the plaintiffs failed to establish that the plaintiffs paid for data security through their monthly premiums.

On the other hand, if the plaintiffs adequately alleged that the defendant received payment in exchange for data security services, and that the defendant failed to provide those services, then the elements of an unjust enrichment claim would be established. Simply stated, the plaintiffs paid for something that they did not receive. Therefore, it is inequitable for the defendant to keep the relevant payment. It is arguably not necessary, as the Eighth Circuit suggested in *Kuhns* and *Carlsen*, to prove that any specific portion of the payment was expressly allocated for data security.[60]

ii. Proposed Test for Establishing Enrichment

The main difficulty lies in proving that the plaintiffs paid for data security. The author submits that the courts should be allowed to infer that the plaintiffs paid for data security services from the circumstances even if no specific portion of the payment is earmarked for such services. In particular, the author proposes introducing the following presumption. The plaintiffs are presumed to have paid for data security if the following three elements are satisfied: (1) the defendant is reasonably expected to take data security measures to protect the plaintiffs' personal data; (2) the plaintiffs conferred a benefit on the defendant (the "payment"); and (3) the defendant is reasonably expected to use at least part of that payment to pay for those data security measures.

The first element may be satisfied in several situations. Firstly, the defendant may be reasonably expected to protect the plaintiffs' personal data because it made an express promise to do so. In the absence of an express promise, such reasonable expectation might be inferred from the context.[61] For example, the plaintiffs might argue that data security is objectively essential to the transaction at issue such that a

59. *Id.*

60. Kuhns v. Scottrade, 868 F.3d 711, 718 (8th Cir. 2017); Carlsen v. GameStop, Inc., 833 F.3d 904, 912 (8th Cir. 2016).

61. *See, e.g.*, *In re* Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 541, 534–45 (M.D. Pa. 2021) (referring to cases where the plaintiffs referenced company-specific documents and policies to support an implied promise to secure the plaintiffs' personal data.). The court also noted that "the context in which a consumer entrusts data to a merchant may be more suggestive of a promise to secure that data than in an employer-employee relationship." *Id.* at 536.

reasonable plaintiff would not have entered into the transaction if the defendant did not provide adequate data security. The plaintiffs can support such argument by showing, for example, that misuse of the type of personal data likely to be transferred in connection with the products/services purchased can cause significant harm to the plaintiffs. Whether a court will make such an inference will depend on the circumstances of the case, especially the amount and sensitivity of the personal data in question. For example, to purchase a medical insurance policy, an individual is often required to transfer to the seller a considerable amount of high-risk personal data (e.g., medical history, credit card information, contact details, and Social Security number), which, if in the wrong hands, could cause significant harm to that individual. As such, the individual likely would not purchase a policy from a seller who does not provide adequate security for her data. In such cases, the court should be more prepared to conclude that the defendant is reasonably expected to safeguard that data. In fact, given the prevalence of data breach incidents, an increasing number of courts have entertained arguments on an implicit contractual duty to safeguard customer personal data.[62] For example, in *Anderson v. Hannaford Bros. Co.*,[63] the First Circuit concluded that when a plaintiff used a credit card to make a purchase from the defendant, a jury could reasonably conclude that "an implicit agreement to safeguard the data [was] necessary to effectuate the contract."[64] For the avoidance of doubt, the plaintiffs do not necessarily have to establish a *contractual* promise to secure personal data to bring an unjust enrichment claim. Finally, a defendant may be reasonably expected to protect the plaintiffs' personal data because the defendant is required by law to do so.[65]

The second element is clearly satisfied where the plaintiffs transferred money (or money equivalent) to the defendant. However, if the defendant only received personal data about the plaintiffs, some courts might be reluctant to conclude that

---

62. *See, e.g.*, Anderson v. Hannaford Bros. Co., 659 F.3d 151, 158–59 (1st Cir. 2011), *cited with approval in In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014). Other cases where the court found that the plaintiffs plausibly alleged the existence of an implied term or implied contract include Irwin v. Jimmy John's Franchise, LLC, 175 F. Supp. 3d 1064, 1070 (C.D. Ill. 2016) ("When the customer uses a credit card for a commercial transaction, he intends to provide the data to the merchant, and not to an unauthorized third party . . . There is an implicit agreement to safeguard the customer's information to effectuate the contract.") (internal citations omitted); *In re* Brinker Data Incident Litig., No. 18-cv-686, 2020 U.S. Dist. LEXIS 247918, at *17 (M.D. Fla. Jan. 27, 2020) ("'The majority of federal courts have held that the existence of an implied contract to safeguard customers' data could reasonably be found to exist between a merchant and customer when a customer uses a payment card to purchase goods and services."); *In re* Marriott Int'l, Inc., 440 F. Supp. 3d 447, 486 (D. Md. 2020) (allowing an implied breach of contract claim under Oregon law); *In re* Rutter's, 511 F. Supp. 3d at 533–37. Compare cases where the court did not find such an implicit contractual duty: Lovell v. P.F. Chang's China Bistro, Inc., No. C14-1152, 2015 U.S. Dist. LEXIS 112101, at *15–16 (W.D. Wash. Mar. 27, 2015) (finding no implied promise to safeguard the plaintiff's card information where the defendant accepted payment via a credit or debit card); *In re* Zappos.com, Inc., No. 12-cv-00325, 2013 U.S. Dist. LEXIS 128155, at *15–16 (D. Nev. Sep. 9, 2013) ("[S]tatements on Zappos's website [that] indicated that its servers were protected by a secure firewall and that customers' data was safe" were insufficient to create any contractual obligations); Wallace v. Health Quest Sys., 20 CV 545, 2021 U.S. Dist. LEXIS 54557 at *1, *27–28 (S.D. Fla. Mar. 23, 2021).

63. *Anderson*, 659 F.3d 151.

64. *Id.* at 159.

65. *See, e.g.*, McGeveran, *supra* note 14, 1143–57.

this element is satisfied on the basis that personal data does not have any independent monetary value.[66] Nevertheless, the author takes the view that, as long as the relevant personal data is of economic value to the defendant, the second element should be satisfied.

To satisfy the third element, the data security services that the defendant is reasonably expected to provide must be sufficiently material that reasonable persons, circumstanced as the actual parties were, would understand that those services are not gratuitous. Several factors are likely relevant. For example, the cost of the relevant data security services must not be negligible such that the defendant can be reasonably expected to charge for them.[67] Moreover, data security must be sufficiently material to the transaction at issue such that the plaintiffs are likely willing to pay for it. There is increasing empirical evidence that people are willing to pay a premium for data protection. For example, researchers found in a lab experiment that a substantial proportion of the participants were willing to pay more (roughly fifty cents more for products costing about fifteen dollars) to purchase products from merchants with more protective privacy policies.[68] Besides, the very fact that many people purchased credit monitoring services after a data breach suggests that they are likely willing to pay for data security services to reduce the likelihood of a data breach in the first place.

However, it may not always be possible for the plaintiffs to allege that any specific portion of their payment is dedicated to data security, particularly in the absence of an express promise to that effect. The failure to do so arguably should not by itself prevent the plaintiffs from establishing an unjust enrichment claim, contrary to the conclusions reached in *Kuhns* and *Carlsen*.[69] These cases highlight the practical difficulty of determining the value of data security, especially where parties have not expressly assigned a dollar amount to it. However, this difficulty can be addressed by presuming that the plaintiffs paid a reasonable amount for data security. What is reasonable depends on the circumstances, such as (a) the price of the products/services purchased by the plaintiffs from the defendant and (b) the cost of reasonable data security measures in a particular case. The court may also be assisted by empirical studies that assess individuals' willingness to pay for data security. It is suggested that, while the valuation difficulties are not trivial, they may not be so insurmountable as to justify an outright denial of an otherwise plausible

---

66. *See, e.g.*, Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 755 (W.D.N.Y. 2017) ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value.") (quoting Welborn v. Internal Revenue Serv., 218 F. Supp. 3d 64, 78 (D.D.C. 2016)).

67. *See, e.g.*, *In re Rutter's*, 511 F. Supp. 3d at 538 ("[C]onsidering the fact that Rutter's has previously acknowledged its efforts to maintain and protect customer data, it is plausible that the cost of data security is baked into its prices.").

68. Janice Y. Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RSCH. 254–68 (2011).

69. A number of district courts also dismissed unjust enrichment claims on this basis. *See, e.g.*, Jurgens v. Build.com, Inc., No. 17-cv-00783, 2017 U.S. Dist. LEXIS 186999, at *17 (E.D. Mo. Nov. 13, 2017) ("But Plaintiff does not allege any facts giving rise to a reasonable inference that any specific portion of the money she paid was intended or required to be spent on data protection. As such, Plaintiff has failed to state a claim that she conferred a benefit on Defendant the retention of which would be inequitable."); Perdue v. Hy-Vee, Inc., 455 F. Supp. 3d 749, 766 (C.D. Ill. 2020) ("Plaintiffs have not alleged that any specific portion of their payments went toward data protection.").

unjust enrichment claim.[70] At least one federal court found it "too much" to require allegations of "a particular sum of the purchase price being explicitly allocated for data security" at the pleading stage.[71] It is worth noting that the proposed presumption (i.e., that the plaintiffs paid reasonable sums for data security) is unlikely to unduly prejudice the defendant's interests because the defendant can always adduce evidence to rebut the presumption and demonstrate that it did not charge for data security. The defendant has intimate knowledge of its own pricing strategy and therefore should be well-positioned to provide such evidence.

Several other grounds for concluding that the defendant has not been enriched are equally unpersuasive. Several courts held that the plaintiffs, as paid customers, did not pay for data security because they received the same data security services as non-paid customers.[72] For example, in concluding that the plaintiffs did not bargain for data security in *Carlsen*, the Eighth Circuit also pointed to their failure to allege that "[the defendant] agreed to provide additional protection to paid subscribers that it did not also provide to non-paid subscribers."[73] The implicit assumption of this reasoning is that customers who received "free" services did not pay for them. This reasoning is specious: as the court recognized in *In re Marriot International Inc. Customer Data Security Breach Litigation*, many customers pay for goods and services with their personal data, rather than cash.[74] In many cases, the more reasonable assumption is that both groups of customers—one paid with both money and data, one paid only with data—have intended a portion of their payment to cover data security.[75] In addition, there is emerging empirical evidence that individuals who paid money for products/services are more likely to have intended that part of their money goes to data security. As researchers found in a recent

---

70. Similar valuation difficulties arise in other contexts. For a critique of the use of conjoint analysis for the purposes of assessing the appropriate damages for breach of data security, see Mike Kheyfets, *Benefit of the But-For Bargain: Assessing Economic Tools for Data Privacy Litigation*, 23 J. TECH. L. & POL'Y 115 (2018).

71. *In re* Intel Corp. CPU Mktg., Sales, Pracs. and Prods. Liab. Litig., No. 18-md-2828, 2020 U.S. Dist. LEXIS 53829, at *23–24 (D. Or. Mar. 27, 2020). *See also In re Eskenazi Health Data Incident Litig.*, No. 49D01-2111, Ind. Super. LEXIS 130, at *29 (Ind. Super. Ct. Sep 2, 2022) ("The Court agrees with Plaintiffs that it is not necessary to specify which portion of the payments account for data security services at this stage of proceedings, only that some portion of it is alleged to have been so directed."). In a different context, a district court refused to follow *Carlsen* and held that the plaintiffs did not have to specify what portion of their premiums went towards data security to recover benefit of the bargain losses for breach of contract. *See In re* Anthem, No. 15-md-02617, 2016 U.S. Dist. LEXIS 70594, at *128 (N.D. Cal. May 27, 2016).

72. *See, e.g.*, *In re* LinkedIn Priv. Litig., 932 F. Supp. 2d 1089, 1093 (N.D. Cal. 2013) (rejecting plaintiffs' overpayment theory of standing because LinkedIn's User Agreement and Privacy Policy were the same for the premium (paid) membership as they were for the basic (free) membership, and the complaint "[did] not sufficiently demonstrate that included in Plaintiffs' bargain for premium membership was the promise of a particular (or greater) level of security that was not part of the free membership."); Carlsen v. GameStop, Inc., 833 F.3d 855, 912 (D. Minn. 2015).

73. *Carlsen*, 833 F.3d at 912.

74. *In re* Marriott Int'l, Inc., 440 F. Supp. 3d 447, 462 (D. Md. 2020).

75. The plaintiff has to overcome the difficulty of showing that her personal data has some ascertainable economic value, which some courts appear reluctant to accept. *See supra* notes 9 and 66.

survey of 1,000 Android mobile app users, individuals were "more likely to expect the paid version [of an app] to engage in privacy-protective practices."[76]

Another version of this argument holds that the plaintiffs did not pay the defendant to secure their credit card information because they paid the same price for a product or service as other customers who paid in cash.[77] However, a plausible objection to this argument is that customers who paid with credit card in fact paid more—they paid with both money and personal data.[78]

Moreover, where a defendant merely promised to comply with data privacy laws, the court has refused to find a tacit agreement to secure the plaintiffs' personal data for remuneration, presumably because the defendant was required by law to provide data security in any event.[79] However, a legal obligation to secure personal data does not in any way prevent a defendant from charging its customers for those required security services. If anything, the existence of such mandatory obligations makes it more likely that the cost of those obligations is baked into the purchase price.

In summary, in determining whether the defendant has been enriched, the court should focus on whether the defendant received payment in exchange for data security services.

b. At the Plaintiff's Expense

The "at the plaintiff's expense" requirement limits the categories of persons who can bring an unjust enrichment claim against a particular defendant. The courts have formulated this requirement in various ways.[80] Some courts require a

---

76. Kenneth A. Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On & Irwin Reyes, *Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps*, 35 BERKELEY TECH. L.J. 327, 327–28 (2020).

77. *See, e.g.*, Gordon v. Chipotle Mexican Grill, Inc., No. 17-cv-1415, 2018 U.S. Dist. LEXIS 129928, at *10 (D. Colo. Aug. 1, 2018) ("[T]hey do not address the reasonable inference that a cash customer—who gives no PII [Personal Identifiable Information] to Defendant in a purchase—would pay lower prices than Plaintiffs if their overpayment assertion were plausible."); *In re* Brinker Data Incident Litig., 2020 U.S. Dist. LEXIS 247918, at *31–32 (M.D. Fla. Jan. 27, 2020) (distinguishing *Resnick* on the basis that it was a data breach in the healthcare context; *id.* ("In a normal consumer transaction (like the ones at issue here), the price is the same regardless of the payment method, yet only customers using payment cards are at risk of having their personal data compromised. Thus, because the customers must have paid only what the good or service was worth, and nothing more, they conferred no additional benefit upon the defendant.") (citation omitted); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014) ("If Target charged credit-and debit-card customers more for their purchases to offset the costs of data security, Plaintiffs might have a plausible allegation in this regard."); Irwin v. Jimmy John's Enter., LLC, 175 F. Supp. 3d 1064, 1071–72 (C.D. Ill. 2016).

78. If the defendant cannot derive any value from that data, they can simply delete it. This in turn protects the defendant from liability for data breach.

79. *See, e.g.*, Brush v. Miami Beach Healthcare Grp. Ltd., 238 F. Supp. 3d 1359, 1369 (S.D. Fla. 2017) ("Nothing in the Plaintiff's Complaint gives rise to a factual inference that the Defendants tacitly agreed to secure her personal data in exchange for remuneration. It is clear from the Plaintiff's allegations that she transacted to receive healthcare services from the Defendants—not data security services beyond the privacy requirements already imposed on the Defendants by federal law. Accordingly, the Court cannot imply a contract to provide data security services based on the conduct of the parties.").

80. This is not surprising. In other common law jurisdictions, legal scholars have struggled to provide a satisfactory definition of this requirement. *See* Stephen Watterson, *At the Claimant's Expense*,

connection between the parties which is "not too attenuated," and refuse to find such a connection where the parties "simply had no dealings with each other."[81] Some require proof of "a connection between the enrichment and the impoverishment."[82] Other courts emphasize that the plaintiff must confer a "direct benefit" on the defendant.[83]

The "at the plaintiff's expense" requirement is invariably satisfied where the plaintiffs make payment to the defendant directly.[84] Plaintiffs may also be able to establish a sufficient connection to satisfy this requirement even if they do not have a direct contractual relationship with the defendant.[85] For example, in *In re Anthem, Inc. Data Breach Litigation*, the defendant, Anthem, Inc., was a large health insurance company, which maintained a computer database containing the personal data of its current and former members.[86] The plaintiffs alleged that Anthem failed to implement basic industry-accepted data security tools, which allowed cyber-attackers to extract massive amounts of data from its database.[87] Some of those plaintiffs did not contract directly with Anthem; instead, they were covered by Administrative Service Only (ASO) agreements between their employers and Anthem.[88] According to the court, it did not matter that those plaintiffs' premiums were aggregated by their respective employers, who then paid Anthem; it was sufficient that Anthem "knew or should have known that some portions of [those plaintiffs'] insurance expenses had been paid by the premiums that [they] paid."[89] Similarly, in *In re Capital One*, the plaintiffs were allowed to pursue an unjust enrichment claim based on overpayment for data security against Amazon even though there were no express contracts between them.[90]

Some courts also require the plaintiffs to show that they suffered pecuniary loss to satisfy the "at the plaintiff's expense" requirement.[91] This requirement might

---

in RESEARCH HANDBOOK ON UNJUST ENRICHMENT & RESTITUTION 262–90 (Elise Bant, Kit Barker & Simone Degeling eds., 2020).

81. *See, e.g.*, Georgia Malone & Co., Inc. v. Rieder, 19 N.Y.3d 511, 517–18 (N.Y. App. Div. 2012), *cited with approval in In re* Anthem, No. 15-md-02617, 2016 U.S. Dist. LEXIS 70594, at *172–73 (N.D. Cal. May 27, 2016).

82. *See, e.g.*, Zuger v. N.D. Ins. Guar. Ass'n, 494 N.W.2d 135, 138 (N.D. 1992); USA Disaster Recovery, Inc. v. St. Tammany Parish Govt., 145 So. 3d 235, 235 n.1 (La. 2013).

83. *See, e.g.*, Weinberg v. Advanced Data Processing, Inc., 147 F. Supp. 3d 1359, 1368 (S.D. Fla. 2015); Peschmann v. Quayle, No. 17-cv-00259, 2019 U.S. Dist. LEXIS 137468, at *48 (W.D. Pa. Aug. 13, 2019).

84. Though proof of direct payment is not necessary to satisfy this requirement.

85. *See, e.g.*, *In re* Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 488, 412 (E.D. Va. 2020); *In re Anthem*, 2016 U.S. Dist. LEXIS 70594, at *90; *Weinberg*, 147 F. Supp. 3d at 1368.

86. *In re Anthem*, 2016 U.S. Dist. LEXIS 70594, at *90.

87. *Id.* at *92–93.

88. *Id.* at *173.

89. *Id.* at *174.

90. *In re Capital One*, 488 F. Supp. 3d at 412 ("There is no express contract between Plaintiffs and Amazon; and courts have concluded that the failure to secure a party's data can give rise to an unjust enrichment claim where a defendant accepts the benefits accompanying plaintiff's data and does so at the plaintiff's expense by not implementing adequate safeguards, thereby making it 'inequitable and unconscionable' to permit defendant to retain the benefit of the data (and any benefits received therefrom).").

91. *See, e.g.*, Cousineau v. Microsoft Corp., 992 F. Supp. 2d 1116, 1130 (W.D. Wash. 2012) ("Cousineau focuses unduly on the benefit to Microsoft despite the fact that she must allege not only that Microsoft benefited but also that she herself was deprived in terms of payment, property, services,

present a problem where the plaintiffs paid the defendant only with personal data, rather than money, in which case the plaintiffs may have difficulty establishing that they have suffered pecuniary loss due to a diminution in value of their personal data.[92]

c. Enrichment is Unjust

Lastly, the plaintiffs must also establish that the defendant has received the benefit in circumstances that make it inequitable for the defendant to retain the benefit. If a defendant failed to take any data security measure, then it is clearly inequitable for the defendant to retain the payment received for data security. Similarly, if a defendant promised to spend 5% of the money received from the plaintiffs on data security, but in fact only spent 2% of the money on such security, then it is inequitable for the defendant to retain the remaining 3%.

Even if a defendant incurred expenses in providing data security services, the quality of those services might be so poor that it is of little to no value to a reasonable person in the plaintiff's position. In such cases, the plaintiffs may argue that the defendant nevertheless failed to provide the data security services reasonably expected from the defendant because its performance was so defective. As a result, it is inequitable for the defendant to retain the payment received for data security. Whether a defendant's performance is sufficiently defective to render it *unjust* to retain payment for data security often depends on the actual content of the promise to provide data security (if any) and on the prevailing standards of data security for a particular industry.[93] The mere fact that the defendant suffered a data breach does not necessarily mean that the defendant failed to take reasonable security measures.[94] Defective performance might be found, for example, in a case where a defendant incurs costs installing security software on company devices in which the plaintiffs' personal data is stored, but knowingly allows its employees to store and transmit that data using unprotected personal devices. The plaintiffs might in turn argue that the defendant's data security measures are defective since they can be so easily circumvented. The plaintiffs therefore cannot be reasonably expected to pay for them.

3. The Case for Embracing the Overpayment Theory of Unjust Enrichment

There are several reasons for embracing the overpayment theory of unjust enrichment as proposed in this Article.

---

or some equivalent form of an expense."). *Cf.* Perlin v. Time Inc., 237 F. Supp. 3d 623, 643 (E.D. Mich. 2017) ("It is evident from these cases that 'loss' is not an element of an unjust enrichment claim under Michigan law.").

92. *See supra* notes 4, 9, and 66.

93. After examining fourteen frameworks that impose data security, William McGeveran concludes there is likely a relatively clear common set of standards for data security in the United States. *See* McGeveran, *supra* note 14.

94. *See, e.g.*, Griffey v. Magellan Health Inc., 562 F. Supp. 3d 34, 50 (D. Ariz. 2021) ("As a matter of logic, however, the existence of an adequate data security infrastructure and two data breaches in a year are not mutually exclusive.").

a. Fair and Intuitive

The first reason is simple. If a plaintiff paid the defendant for data security services, but did not receive them, then it is unfair for the defendant to keep that payment.

Some of the cases adopting the overpayment theory of unjust enrichment have also pointed to the fact that the plaintiffs would not have purchased products or services from the defendant had they known that the defendant would not adequately protect their personal data.[95] That causal link certainly supports the overpayment theory of unjust enrichment. However, a failure to allege such a link should not preclude an unjust enrichment claim based on overpayment. Once a court concludes that the plaintiffs paid for something that they did not get, that alone should be sufficient to support an unjust enrichment claim.

b. Incentivizes Responsible Data Security Practice

Second, the overpayment theory of unjust enrichment highlights the importance of data security. It proceeds on the basis that individuals who transfer certain types of personal data to a company, in connection with products/services provided, take their privacy seriously enough to pay for reasonable data security services. This is often a fair assumption in light of the rapid increase in data breach incidents around the world.[96] Plaintiffs who have fallen victim to a data breach suffer real harms.[97] There is a higher chance that their personal data will be used against their interests: wrongdoers might use that data to locate and injure them[98] or to purchase goods and services in their names.[99] Whether or not the risk of data misuse materializes, the plaintiffs are likely to feel anxious and stressed about the possibility of such misuse. They might also incur time and expenses to take preventive steps to identify (e.g., by subscribing to credit-monitoring services) or to prevent data misuse (e.g., by cancelling credit cards).[100]

The overpayment theory of unjust enrichment clearly incentivizes defendants to take reasonable data security measures since they cannot profit by skimping on data security.[101] If they fail to provide adequate data security, they are required to return the payment made for those services. By contrast, if liability for taking inadequate data security is conditioned on proof of damages suffered by the plaintiffs, then a defendant might sometimes find it cost-effective to take little or no data security measures because it is often difficult for plaintiffs to demonstrate

95. *See, e.g.*, *In re Capital One*, 488 F. Supp. 3d at 404, 412.

96. *See, e.g.*, Bree Fowler, *Data Breaches Break Record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ [https://perma.cc/QM2W-XVVG].

97. *Risk and Anxiety*, *supra* note 16, at 750–54.

98. For example, victims of domestic abuse might be worried that unauthorized disclosure of personal identifying information will enable their former abusers to find them. *See* Doe v. Compact Info. Sys., No. 13-cv-5013, 2015 U.S. Dist. LEXIS 178930, at *18–19 (N.D. Tex. Jan. 26, 2015).

99. *See, e.g.*, Irwin v. Jimmy John's Enter., LLC, 175 F. Supp. 3d 1064, 1073–74 (C.D. Ill. 2016).

100. For more details, see *infra* Section II.B.1.

101. In a similar context, Bernard Chao also argued that awarding the disgorgement remedy for breach of data security promises would encourage companies to take such promises more seriously. *See* Chao, *supra* note 3, at 579.

that they have suffered actual loss as a result of a data breach.[102] If only a limited number of plaintiffs are able to prove their loss at court, some defendants might conclude that it is cheaper to pay for those plaintiffs' loss than to take adequate security measures.

c. Easy to Establish Constitutional Standing

Another major challenge for data breach victims is to establish constitutional standing. To bring a claim in a federal court, a plaintiff must show "(i) that he suffered an *injury in fact* that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief."[103]

Much ink has been spilled on the seemingly inconsistent approaches taken by appellate courts with respect to constitutional standing in data breach cases.[104] Briefly stated, some courts are reluctant to confer standing on plaintiffs who have not yet suffered any data misuse, particularly if they fail to show that at least some victims of the same data breach have already experienced data misuse.[105] In response, commentators argue, for example, that courts should recognize a greater variety of privacy harms (e.g., increased risk of harm).[106]

By contrast, plaintiffs pursuing an unjust enrichment claim for overpayment of data security do not have to persuade the courts to recognize new types of harm. As long as there is sufficient evidence that the plaintiffs paid for data security, which the defendant failed to provide, the plaintiffs should have little difficulty establishing that they suffered financial harm in the form of overpayment. Financial harm clearly qualifies as *injury in fact*.[107] This injury is caused by the defendant's failure to perform the data security services reasonably expected from it and can be readily redressed by requiring the defendant to return the amount overpaid. As such, the plaintiffs should be able to establish constitutional standing to bring their unjust enrichment claims.

4. The Unjust Enrichment Cause of Action is Not Redundant

A possible argument against recognizing unjust enrichment claims based on overpayment for data security is that such claims can invariably be recast as claims for breach of contract and are therefore redundant. To establish the proposed unjust enrichment claim, plaintiffs might seek to show that the defendant made an express or implied data security promise.[108] If this promise is contained in a contract between the parties, then data breach victims can sue the defendant for breach of the contractual promise to secure data. Indeed, plaintiffs have sought to recover "lost benefit of the bargain" damages for breach of contract in data breach cases to recover the difference between the price of the products/services paid and the

102. *See supra* Introduction and note 4; *infra* Section II.B.1 and Section II.B.2.
103. TransUnion, LLC v. Ramirez, 141 S. Ct. 2190, 2203 (2021).
104. *See, e.g.*, Thomas D. Haley, *Data Protection in Disarray*, 95 WASH. L. REV. 1193 (2020).
105. *See supra* Introduction and note 12.
106. *Risk and Anxiety*, *supra* note 16; *Privacy Harms*, *supra* note 16.
107. *TransUnion*, 141 S. Ct. at 2204.
108. *See supra* Section I.A.2.a.ii.

lower value of the products/services they actually received (due to the defendant's failure to provide adequate data security).[109]

Instead of proving that unjust enrichment claims based on overpayment for data security are redundant, this argument shows that unjust enrichment claims are particularly useful in at least two related situations.

Firstly, there may not always be a *contractual* promise to protect the plaintiffs' personal data.[110] Without such a promise, the plaintiffs can still pursue unjust enrichment claims, which do not require the plaintiff to be "in privity with the defendant."[111] For example, in *In re Anthem*, several plaintiffs did not have a direct contractual relationship with Anthem. Instead, their employers entered into ASO agreements with Anthem and paid Anthem insurance premiums pursuant to those agreements.[112] Some of those plaintiffs unsuccessfully sought to sue Anthem for breach of contract as third-party beneficiaries.[113] Other plaintiffs, as mentioned above, were able to sue Anthem for unjust enrichment.[114] Secondly, where the contracts between the parties are invalid, voidable, or otherwise unenforceable,[115] the plaintiffs can nevertheless rely on unjust enrichment as a cause of action to recover overpayment for data security.

The more difficult question (considered in Part III.A) is whether data breach victims should be allowed to pursue unjust enrichment claims where there is a valid and subsisting contract governing the subject matter of the dispute. This author concludes that arguably unjust enrichment claims should still be permitted in those cases provided that they do not undermine the contractual allocation of risk.

B. The "Would Not Have Shopped" Theory of Unjust Enrichment

The alternative, "would not have shopped" theory of unjust enrichment, which has been applied in a number of data breach cases, is potentially more confusing.

1. In re Target Corp.

Resnick was distinguished in *In re Target Corp. Data Security Breach Litigation*, which allowed the plaintiffs' unjust enrichment claim to proceed on a different theory.[116] In *In re Target*, hackers stole personal data, including credit and debit card

---

109. *See, e.g.*, *In re* Anthem, No. 15-md-02617, 2016 U.S. Dist. LEXIS 70594, at *128 (N.D. Cal. May 27, 2016) ("Plaintiffs may be able to recover benefit of the bargain losses" for breach of contract)*; see also* Kheyfets, *supra* note 70.

110. *See supra* Introduction and note 7. For example, in *In re Capital One Consumer Data Security Breach Litigation*, 488 F. Supp. 3d 374, 412 (E.D. Va. 2020), "there is a fundamental dispute between the parties concerning the scope of [their] contractual relationship and whether it definitively defines [the defendant's] obligations with respect to protecting Plaintiffs' PII."

111. *See, e.g.*, *In re Anthem*, 2016 U.S. Dist. LEXIS 70594 at *173.

112. *Id.* at *136.

113. *Id.* at *137–39 (holding the relevant ASO agreements expressly disclaimed third-party beneficiary status).

114. *See supra* Section I.A.2.b. It is unclear, however, whether those plaintiffs' ASO agreements expressly disclaimed third party beneficiary status.

115. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 2 cmt. c (AM. L. INST. 2011).

116. 66 F. Supp. 3d 1154, 1177–78 (D. Minn. 2014).

information, of about 110 million Target customers.[117] A group of customers brought a putative class action against Target for negligence in failing to safeguard their personal data, breach of contract, breach of privacy and consumer protection statutes, and unjust enrichment.[118] With respect to unjust enrichment, the court distinguished *Resnick* on the basis that every plaintiff in that case "paid the allegedly increased charge for data security because every member's personal information was at risk from insufficient security."[119] But the same was not true for Target, which charged the same price whether a customer paid in cash or by credit/debit card.[120] As argued above,[121] this factor alone should not necessarily entail a finding that the defendant was not enriched. Having rejected the overpayment theory, the court held that the plaintiffs plausibly alleged an unjust enrichment claim based on the "would not have shopped" theory.[122] That is, had Target notified the plaintiffs of the data breach in a timely manner, they would not have shopped at Target and thus any money they spent at Target was money which Target "in equity and good conscience" should not have received.[123]

In re Target has been cited with approval by the Eighth Circuit in *Carlsen* and by various district courts.[124] In at least one case, *In re Brinker*, the court preferred *In re Target*'s "would not have shopped" theory to *Resnick*'s overpayment theory, narrowly construing the latter as applicable only in the healthcare context.[125]

2. Unpacking the "Would Not Have Shopped" Theory

This Section considers the necessary elements for establishing an unjust enrichment claim based on the "would not have shopped" theory. As noted above,[126] to bring an unjust enrichment claim, a plaintiff must establish that the defendant has received benefits "under circumstances making it inequitable for the defendant to retain the benefit[s]."[127] The defendant has clearly received benefits at the plaintiff's expense where the plaintiffs purchase products or services from the defendant. The other two elements—enrichment and unjustness—deserve further elaboration.

---

117. *Id.* at 1157.

118. *Id.* at 1157–58. Plaintiffs also brought a claim for bailment, which was dismissed.

119. *Id.* at 1178.

120. *Id.*

121. *See supra* Section I.A.2.a.ii.

122. 66 F. Supp. 3d at 1178.

123. *Id.*

124. *See, e.g.*, Baldwin v. Nat'l W. Life Ins. Co., No. 21-cv-04066, 2021 U.S. Dist. LEXIS 175229, at *24 (W.D. Mo. Sept. 15, 2021); *In re* Brinker Data Incident Litig., No. 18-cv-686, 2020 U.S. Dist. LEXIS 247918, at *31–32 (M.D. Fla. Jan 27, 2020); *In re* Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 514, 538 (M.D. Pa. 2021); *In re* Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 412 (E.D. Va. 2020); Carlsen v. GameStop, Inc., 112 F. Supp. 3d 903, 861 (8th Cir. 2016); Gordon v. Chipotle Mexican Grill, Inc., No. 17-cv-1415, 2018 U.S. Dist. LEXIS 129928, at *10 (D. Colo. Aug. 1, 2018).

125. *In re Brinker*, 2020 U.S. Dist. LEXIS 247918, at *31–33 ("However, no court has extended this theory to data breach cases outside of the healthcare context."). In *In re Brinker*, the plaintiffs argued that they would not have dined at restaurants owned by Brinker had they known that Brinker would not adequately secure their data. *Id.* at *33.

126. *See supra* Section I.A.

127. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 cmt. d (AM. L. INST. 2011).

a. Enrichment Is Unjust

The plaintiff may argue that it would be inequitable for the defendant to retain certain benefits received from the plaintiff because the transfer was induced by invalidating mistake. Section 5(1) of the Restatement (Third) of Restitution and Unjust Enrichment (hereinafter referred to as the "*Restatement*") provides that "[a] transfer induced by invalidating mistake is subject to rescission and restitution. The transferee is liable in restitution as necessary to avoid unjust enrichment." Moreover, there is invalidating mistake only when "(a) but for the mistake the transaction in question would not have taken place; and (b) the claimant does not bear the risk of the mistake."[128] Therefore, a plaintiff must establish that she transferred benefits (in the form of money or personal data) to the defendant due to a mistake (e.g., a mistake about the defendant's actual data security practice) and that she would not have conferred those benefits but for the mistake. The mistake does not have to have been created or induced by the defendant.[129] As the court recognized in *In re Target*, the presence of a causative mistake can arguably be found where the plaintiff would not have transferred money to the defendant (e.g., by not purchasing any product or service) had she known about the defendant's inadequate data security.[130]

b. Enrichment

The extent of the defendant's enrichment under the "would not have shopped" theory is less clear. The defendant is only enriched by the amount of benefit that the plaintiffs would not have conferred had they known about the defendant's inadequate data security. Thus, the plaintiffs might argue that they conferred two types of benefits on the defendant:

(1) a portion of the purchase price that the defendant should have spent on data security, if the plaintiffs can show that the cost of data security was likely baked into the purchase price; and

(2) the amount of benefit that the defendant received by using the plaintiffs' data transferred in connection with that purchase.[131]

If the plaintiffs seek to recover the first type of enrichment, then their claim can invariably be recast as a claim based on overpayment for data security (i.e., the defendant received payment for data security, but failed to provide adequate data security services). Indeed, in such cases, the overpayment theory arguably provides a more straightforward explanation as to why it is unjust for the defendant to retain the payment intended for data security than the "would not have shopped" theory. Additionally, as explained below,[132] claims based on the overpayment theory are more amenable to class action resolution.

---

128. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 5 (AM. L. INST. 2011).

129. *Id.*

130. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014).

131. *See, e.g.*, *In re Brinker*, No. 18-cv-686, 2020 U.S. Dist. LEXIS 247918, at *34 (M.D. Fla. Jan 27, 2020).

132. *See infra* Section II.B.2.

If the plaintiffs seek to recover the second type of enrichment, the situation is slightly more complicated. A court must first determine whether the defendant has indeed benefited from using the plaintiffs' personal data.[133] Companies can benefit from the data they have collected in many ways: they might sell that data, use it to generate additional insights about their customers, or use it to improve their products or develop new ones. However, it may not always be easy to ascertain the exact benefit received by the defendant from using personal data about the plaintiffs. It is submitted that, in assessing the amount of benefit received from such use, the court may be assisted by considering the following factors. Firstly, if the defendant has sold the data, then the sale price helps determine the value of that data. Secondly, if the defendant has received benefits or saved costs as a result of using the plaintiffs' personal data, then the use value of that data may be measured by reference to the amount of that benefits or costs saved.[134] For example, such data might help companies save costs in conducting experiments for the purpose of determining how to increase user engagement or determining how to optimize advertisement sales.[135] Another example is where the defendant benefits from storing the plaintiffs' personal data by charging third parties for its services.[136] Finally, there might occasionally exist a market price or independent studies about the value of certain types of personal data, which are similar to the type of data used by the defendant.[137] Such studies can in turn shed light on the use value of the data in question.

The court will then need to determine the extent to which the defendant's use of personal data is permitted under the contract between the parties (if any). If the relevant use is prohibited under the contract (e.g., the defendant may have expressly represented that it would not use the plaintiffs' data for marketing purposes), then the plaintiffs might argue that they made an invalidating mistake when they transferred their data. They were mistaken as to the purpose for which their data would be used and would not have transferred their data had they known the true purpose. If the most appropriate interpretation of the contract is that the relevant use is permitted provided that certain conditions are satisfied (e.g., that the defendant provides adequate data security), then the plaintiffs might argue that they made a mistake as to the defendant's data security practice and that they would not have transferred their data had they known the truth. By contrast, if the relevant use is permissible irrespective of the defendant's data security practice, then the

---

133. *See supra* Section I.A.2.a.

134. The defendant might draw a distinction between (1) the plaintiffs' personal data and (2) the use value of that data. It may then rely on *Prudential Assurance Co. v. Revenue and Customs Commissioners* [2018] UKSC 39, [2019] AC 929 (appeal taken from EWCA (Civ)), to argue that the use value of that data should be irrelevant because it is not obtained at the plaintiffs' expense. This type of argument has been criticized by various commentators. *See, e.g.*, Andrew Burrows, *In Defence of Unjust Enrichment*, 78 CAMBRIDGE L.J. 521, 538–41 (2019). The author's preferred view is that the defendant's enrichment should include such use value.

135. Jack Balkin points out that individual users are in effect "unpaid laborers." Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011, 2024 (2018).

136. *See, e.g.*, *In re* Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 413 (E.D. Va. 2020) (noting that Amazon benefited from storing the plaintiffs' personal data by charging Capital One for server use).

137. See, for example, *In re* Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589, 600 (9th Cir. 2020), where the plaintiffs relied on a study which valued users' browsing histories at $52 per year.

plaintiffs are unlikely able to bring any unjust enrichment claims because such claims would undermine the parties' contractual allocation of risk.[138]

c. The Risk-Taker Objection

As noted above,[139] a defendant might seek to defeat a mistake-based unjust enrichment claim by arguing that the plaintiffs bear the risk of their mistake. The defendant might argue, for example, that the plaintiffs suspected that the defendant might not take adequate data security measures, but allowed the defendant to collect their data anyway. In other words, the plaintiffs "consciously assumed the risk by deciding to act in the face of a recognized uncertainty."[140] Whether it is necessary or desirable to have a separate non-risk-taker requirement is questionable in the first place. One might argue that the risk-taker argument does not add anything to the causation requirement, but is merely an example where there is no causative mistake.[141] In any event, a plaintiff is generally not considered a risk-taker simply because she made a mistake as a result of her negligence.[142] As such, evidence that a reasonable person in the plaintiff's position would have discovered the defendant's actual data practice (e.g., by reading the privacy policy) should not in and of itself bar a plaintiff from relying on her mistake to bring an unjust enrichment claim.

C. Applications in Non-Data-Breach Cases

Clarifying the meaning and scope of both the overpayment and "would not have shopped" theories of unjust enrichment is important because plaintiffs have brought unjust enrichment claims to seek redress not only for inadequate data security, but also for use of personal data for a purpose unauthorized by data subjects (without disclosure to third parties),[143] unauthorized disclosure of personal

---

138. For a more detailed discussion of the relationship between contract and unjust enrichment claims, *see infra* Section III.A. In such cases, the plaintiffs are also likely to have difficulty showing that they would not have transferred benefits to the defendant but for their mistake.

139. *See supra* Section I.B.2.a.

140. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 5(4)(b) (AM. L. INST. 2011).

141. Thanks to Rory Gregson for raising this point. This non-risk-taker requirement has been subject to criticism in England, where many unjust enrichment cases also recognize a role for risk-taking analysis where a plaintiff relies on mistake as the ground for bringing an unjust enrichment claim. *See, e.g.*, Kleinwort Benson Ltd. v. Lincoln City Council [1999] 2 AC 349 [410]; Deutsche Morgan Grenfell Group Plc. v. Inland Revenue Comm'rs [2007] 1 AC 558 at [26]–[27], [64]–[65] and [175]. For criticisms of this requirement, see Frederick Wilmot-Smith, *Replacing Risk-Taking Reasoning*, 127 L. Q. REV. 610–16 (2011) (identifying five flaws of risk taker reasoning: "[t]he reasoning is circular, ambiguous, inconclusive, incapable of explaining the decided cases and unnecessary").

142. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 5(4) (AM. L. INST. 2011).

143. *See, e.g.*, McCoy v. Alphabet, Inc., No. 20-cv-05427, 2021 U.S. Dist. LEXIS 24180 (N.D. Cal. Feb. 2, 2021); In re Google Location Hist. Litig., 514 F. Supp. 3d 1147 (N.D. Cal. 2021); Fraley v. Facebook, Inc. 830 F. Supp. 2d 785 (N.D. Cal. 2011); Mitchell v. Wells Fargo Bank, 355 F. Supp. 3d 1136 (D. Utah 2018); Cousineau v. Microsoft Corp., 992 F. Supp. 2d 1116 (W.D. Wash. 2012).

data,[144] and unauthorized collection of personal data.[145] An example of the overpayment theory can be found in *Goodman v. HTC Am. Inc.*, where the court held that the plaintiffs adequately stated an unjust enrichment claim under Washington law.[146] Plaintiffs alleged that they overpaid HTC for smartphones because they would have paid less had they known that those phones collected their fine location data,[147] and that it was unjust for HTC to retain that benefit because HTC profited by "misleading and economically harming" the plaintiffs.[148]

An example of the "would not have shopped" theory can be found in the more recent case of *Hart v. TWC Production and Technology LLC*.[149] The defendant's weather app gained access to Hart's location data by promising to provide personalized weather information.[150] In reality, the app collected "minute-by-minute and sometimes second-by-second" location data, "even when the app was closed, and sold this data to third parties."[151] The court concluded that Hart successfully pleaded an unjust enrichment claim on the basis that he "never agreed to share all his location data with TWC."[152]

Clarifying both theories of recovery can hopefully assist those courts in identifying the essential elements of an unjust enrichment claim more accurately and in resolving unjust enrichment claims at a more substantive stage.

---

144. *See, e.g.*, Wheaton v. Apple Inc., No. C 19-02883, 2019 U.S. Dist. LEXIS 185524 (N.D. Cal. Oct. 25, 2019); Dinerstein v. Google, LLC, 484 F. Supp. 3d 561 (N.D. Ill. 2020); Silver v. Stripe Inc., No. 20-cv-08196, 2021 U.S. Dist. LEXIS 141090 (N.D. Cal. Jul. 28, 2021); *In re* Zoom Video Commc'ns. Priv. Litig., 525 F. Supp. 3d 1017 (N.D. Cal. 2021); Klein v. Facebook, Inc., 580 F. Supp. 3d 743 (N.D. Cal. 2022); Brooks v. Thomson Reuters Corp., No. 21-cv-01418, 2021 U.S. Dist. LEXIS 154093 (N.D. Cal. Aug. 16, 2021); Cottle v. Plaid Inc., 536 F. Supp. 3d 461 (N.D. Cal. 2021); Piper v. Talbots, Inc., 507 F. Supp. 3d 339 (D. Mass. 2020); *In re* Facebook, Inc., 402 F. Supp. 3d 767 (N.D. Cal. 2019); Boelter v. Hearst Commc'ns., Inc., 269 F. Supp. 3d 172 (S.D.N.Y. 2017); *In re* Google Referrer Header Priv. Litig., 869 F.3d 737 (9th Cir. 2017), *rev'd in* Frank v. Gaos, 139 S. Ct. 1041 (2019); Mount v. PulsePoint, Inc., 13 Civ. 6592, 2016 U.S. Dist. LEXIS 112315 (S.D.N.Y. Aug. 17, 2016); *In re* Nickelodeon Consumer Priv. Litig., No. 15-1441, 2014 U.S. Dist. LEXIS 91286 (D.N.J. Jul. 2, 2014); Austin-Spearman v. AARP, 119 F. Supp. 3d 1 (D.D.C. 2015); Coulter-Owens v. Time, Inc., 308 F.R.D. 524 (E.D. Mich. Jul. 27, 2015); Pirozzi v. Apple, Inc., 966 F. Supp. 2d 909 (N.D. Cal. 2013); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010 (N.D. Cal. 2012); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2012); Steinberg v. CVS Caremark Corp., 899 F. Supp. 2d 331 (E.D. Pa. 2012); Wiles v. Worldwide Info., Inc., 809 F. Supp. 2d 1059 (W.D. Mo. 2011); *In re* Facebook Priv. Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011).

145. *See, e.g.*, Goodman v. HTC Am., Inc., No. C11-1793, 2012 U.S. Dist. LEXIS 88496 (W.D. Wash. Jun. 26, 2012); *In re* Vizio, Inc. 238 F. Supp. 3d 1204 (C.D. Cal. 2017); *Dinerstein*, 484 F. Supp. 3d 561; *McCoy*, 2021 U.S. Dist. LEXIS 24180; Hart v. TWC Prod. & Tech. LLC, 526 F. Supp. 3d 592 (N.D. Cal. 2021); *Klein*, 580 F. Supp. 3d 743; *Cottle*, 536 F. Supp. 3d 461; Williams v. Facebook, Inc., 384 F. Supp. 3d 1043 (N.D. Cal. 2018); *In re* Nickelodeon, 2014 U.S. Dist. LEXIS 91286; Harris v. comScore, Inc., 292 F.R.D. 579 (N.D. Ill. Apr. 2, 2013); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040.

146. 2012 U.S. Dist. LEXIS 88496.

147. *Id.* at *4.

148. *Id.* at *47.

149. 526 F. Supp. 3d at 592.

150. *Id.* at 597.

151. *Id.* at 600.

152. *Id.* at 605.

II. UNJUST ENRICHMENT FACILITATES DATA BREACH CLASS ACTIONS

Data breach actions are often brought as class actions because a data breach frequently involves personal data concerning a large number of people and because the losses suffered by most individuals are too small to justify bringing individual lawsuits. However, the existing literature on unjust enrichment in data breach and other privacy cases has not analyzed the relationship between the unjust enrichment cause of action and class action.[153]

This Part explores several reasons that data breach victims seeking consequential damages in a tort or contract claim have struggled or will likely struggle to prove that their claims satisfy Rules 23(a) and 23(b)(3) of the Federal Rules of Civil Procedure to attain class certification.[154] It also explains, with respect to each reason, why unjust enrichment claims are more likely to satisfy the requirements in those provisions.[155] Finally, this Part argues that although the availability of an unjust enrichment claim likely increases the size of a data breach class action, it is unlikely to result in overdeterrence.

A. Less Divergence of Interests Between Class Members

To be classified as a class action, a claim must satisfy the four threshold requirements of Rule 23(a) of the Federal Rules of Civil Procedure: (1) numerosity, (2) commonality, (3) typicality, and (4) adequacy of representation. Numerosity requires the putative class to be so numerous that joinder is impracticable.[156] Commonality requires that the claim involves "questions of law or fact common to the class."[157] This in turn requires, as the Supreme Court explained in *Wal-Mart Stores, Inc. v. Dukes*,[158] that the claims of all class members "depend on a common contention," which is "capable of classwide resolution."[159] Typicality requires the class representatives' claims to be typical of the claims of the putative class.[160] Finally, adequacy of representation has two components: (1) the class representatives' interests must be aligned with the class's interests, and (2) the class counsel must capably litigate the case.[161]

While the numerosity requirement can be easily satisfied in data breach cases affecting a large number of people, whether the remaining three requirements can

153. Neither Chao, *supra* note 3, nor Scholz, *supra* note 23, discusses this issue. Lior Strahilevitz briefly observes that the Seventh Circuit's refusal to allow data breach victims to pursue an unjust enrichment claim "had the effect of shrinking the size of the class action and substantially reducing the potential liability for firms." Strahilevitz, *supra* note 20, at 2489.

154. There is limited case law on this point since many putative data breach class actions failed at the pleading stage for the various reasons mentioned in the introduction (e.g., failure to establish Article III standing).

155. While this Part focuses on unjust enrichment claims for overpayment for data security, the reasoning may also apply to claims for breach of contractual duties to provide adequate data security. *See supra* Section I.A.4.

156. FED. R. CIV. P. 23(a).

157. FED. R. CIV. P. 23(a)(2).

158. Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338 (2011).

159. *Id.* at 350 ("[W]hich means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke.").

160. FED. R. CIV. P. 23(a)(3).

161. FED. R. CIV. P. 23(a)(4).

be satisfied is less clear. As the Court stated in *General Telephone Co. v. Falcon*,[162] those three related requirements serve as guideposts for determining "whether the named plaintiff's claim and the class claims are so interrelated that the interests of the class members will be fairly and adequately protected in their absence."[163] However, there are some differences in the types of harm that victims of a data breach suffer. Some class members may have suffered actual loss while others seek damages for an increased risk of future injury. Among those who have suffered actual loss, some may have incurred financial loss as a result of identity theft, some may have spent time and money mitigating their exposure, yet others may have endured anxiety and distress. As a result, to the extent that claims other than unjust enrichment are brought, the interests of those victims may not be completely aligned.

The courts have previously declined to certify a class due to disparities in the type of injuries suffered by putative class members. For example, when the Supreme Court refused to approve a class action settlement of asbestos-related claims in *AmChem Products, Inc. v. Windsor*, it concluded that the adequacy of representation was not satisfied due to conflicts of interests between the named plaintiffs, who already suffered medical conditions, and other putative class members, some of whom had not developed symptoms.[164] The most salient conflict, according to the Court, was the divergence of interests between "the currently injured and exposure-only categories of plaintiffs."[165] More recently, in *Dolmage v. Combined Insurance Co. of America*,[166] the plaintiff sought to certify a class action for breach of contract to provide adequate data security. The district court concluded that the commonality and typicality requirements were not satisfied precisely because the putative class members suffered a diverse range of harms,[167] which could not be determined on a class-wide basis.

By contrast, when data breach victims bring an unjust enrichment claim based on overpayment for data security, there is little divergence of interests between those victims.[168] For example, in a claim based on overpayment for data security, all class members claim to have suffered an existing financial harm—they paid for data

162. Gen. Tel. Co. v. Falcon, 457 U.S. 147 (1982).

163. *Id.* at 157–58.

164. AmChem Prods., Inc. v. Windsor, 521 U.S. 591, 610 (1997).

165. *Id.* at 626.

166. *See* Dolmage v. Combined Ins. Co. of Am., No. 14-C-3809, 2017 U.S. Dist. LEXIS 67555 (N.D. Ill. May 3, 2017).

167. As the court noted, "identity theft is by its very nature a highly personalized crime . . . . [O]f the 4,000 plus proposed class members, some (like Plaintiff) may have become the victim of an actual theft of funds. A subset of these, individuals may have been able to resolve the problems quickly or obtain reimbursement from banks and other third parties. Others may have spent months trying to resolve the identity fraud with little or no success, to the point that they 'encounter[ed] employment and relationship issues.' Other class member [sic] may have not had their information stolen by an identity thief but nevertheless incurred minor expenses monitoring their credit or taking other steps to protect themselves. Another subset of class members may have had no out-of-pocket expenses at all, but suffered emotional distress worrying that they could become a victim of identity theft. Still others may have suffered no distress or inconvenience whatsoever." *Id.* at *24–25.

168. *See also* Strahilevitz, *supra* note 20, at 2489 (noting that embracing the unjust enrichment theory of data breaches would ameliorate class conflicts).

security, but did not receive it. Moreover, as argued above,[169] each class member seeks to recover the same type of loss—the actual or reasonable price of data security objectively assessed in light of the totality of circumstances. In a claim based on the "would not have shopped" theory, all class members claim to have transferred personal data to the defendant based on invalidating mistakes and seek to recover the use value of their data.[170] The absence of conflicts of interests among class members has an important implication. There is no need to divide data breach victims into subclasses, each represented by its own attorneys. This in turn reduces the amount of necessary litigation costs for conducting data breach class actions.

B. More Likely to Satisfy the Predominance Requirement

In addition to satisfying Rule 23(a), the claim must also fall within one of the three categories of Rule 23(b).[171] In particular, to obtain pecuniary relief for individual class members,[172] the claim must satisfy the two requirements under Rule 23(b)(3):

> (1) the questions of law or fact common to class members predominate over any questions affecting only individual members (the 'predominance' requirement); and
>
> (2) a class action is superior to other available methods for fairly and efficiently adjudicating the controversy (the 'superiority' requirement).[173]

The superiority requirement should not present a serious challenge in data breach cases. The courts have generally found that a class action is superior where potential damages for each class member are too insignificant for them to pursue an action individually.[174] Since the amount recoverable by individual data breach victims is generally too small to incentivize them to bring individual actions, the superiority requirement should generally be satisfied in data breach cases.[175]

By contrast, the predominance requirement, which is more demanding than the commonality requirement discussed above, poses greater problems for data breaches victims. To satisfy the predominance requirement, the plaintiffs must show that common questions of law or fact predominate over individual questions. An individual question is one which requires individualized evidence from each class

---

169. *See supra* Section I.A.2.a.ii.

170. Here, an argument can potentially be made that there is a conflict of interest between class members because the nature and amount of data transferred by each class member may be slightly different. This conflict may not be sufficiently serious, and the author takes the view that it is often appropriate for each class member to recover the same amount of use value. *See infra* Section II.B.1.c.

171. AmChem Prods., Inc. v. Windsor, 521 U.S. 591, 614 (1997).

172. Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 360 (2011) (holding that where "the monetary relief is not incidental to the injunctive or declaratory relief," a class action cannot be certified under Rule 23(b)(2)).

173. FED. R. CIV. P. 23(b)(3).

174. *See, e.g.*, *Amchem Prods.*, 521 U.S. at 617.

175. *See, e.g.*, *In re* Hannaford Bros., 293 F.R.D. at 33–34 ("Given the size of the claims, individual class members have virtually no interest in individually controlling the prosecution of separate actions.").

member.[176] A common question is one where "the same evidence will suffice for [all class members]" or where "the issue is susceptible to generalized, class-wide proof."[177] As the Advisory Committee that drafted Rule 23(b)(3) stated: "A 'mass accident' resulting in injuries to numerous persons is ordinarily not appropriate for a class action because of the likelihood that significant questions, not only of damages but of liability and defenses of liability, would be present, affecting the individuals in different ways."[178]

In a data breach class action, a defendant may seek to argue that the predominance requirement is not satisfied based on at least three grounds—individualized evidence is required (1) to determine the amount of damages recoverable; (2) to establish causation; and (3) to raise a defense.[179] Each ground is examined in turn.

1. Requires Individualized Evidence to Determine Damages

Firstly, defendants may argue that the predominance requirement is not satisfied because individualized evidence is required to determine the amount of damages recoverable by each putative class member.

a. The Need for Individualized Evidence to Recover Consequential Loss

In data breach cases, plaintiffs have mainly relied on four types of losses to establish the damages element of a tort or contract claim. These include:

(1) loss from data misuse, such as identity theft;

(2) time, effort, and expenses incurred to mitigate the consequences of a data breach, such as the cost of credit monitoring services ('mitigation costs');

(3) emotional distress; and

(4) increased risk of future harm.[180]

For each category of loss, there is likely to be great disparity among data breach victims in such matters as the extent and type of loss suffered. As noted above,[181] personal data disclosed in a data breach can be misused in a myriad of ways. Even assuming all putative class members suffered identity theft perpetrated by the same person, each incident may have occurred at different times and places; different victims may also have sustained different levels of financial loss. Similarly, the amount of time, effort, and expenses incurred to identify and remedy the consequences of a data breach are likely to vary significantly from victim to victim.

176. Tyson Foods, Inc. v. Bouaphakeo, 577 U.S. 442, 453 (2016) (quoting WILLIAM RUBENSTEIN, NEWBERG ON CLASS ACTIONS 196–97 (5th ed. 2012).

177. *Id.*

178. FED. R. CIV. P. 23(b)(3) advisory committee's notes to 1966 amendment.

179. *See generally* Section II.B.

180. For example, in *Dolmage v. Combined Insurance Company of America*, No. 14-C-3809, 2015 U.S. Dist. LEXIS 6824 (N.D. Ill. Jan. 21, 2015), the plaintiffs sought to recover (1) economic losses resulting from identity theft; (2) loss from improper disclosure of personal data; (3) loss of privacy; (4) reasonable expenses and time incurred to remedy identity theft and to mitigate the increased risk of identity theft; and (5) anxiety and emotional distress. *Id.* at *4-5.

181. *See supra* Section I.A.3.b.

Additionally, whether a data breach victim suffers any emotional distress, and the extent of such distress, is likely determined by characteristics unique to each individual.[182] Finally, any increase in risk of future harm suffered by each data breach victim likely depends on their personal circumstances such as privacy preferences and ability to take protective measures.[183] For example, individuals whose relevant data has been subject to multiple data breaches may not experience as significant an increase in risk as individuals whose data has not been so disclosed previously.

Such disparities among data breach victims have two main implications. First, the necessary evidence for establishing the existence and extent of loss suffered by a data breach victim (let us call her Jane) is often possessed only by that victim. Take mitigation costs as an example. Jane, and only Jane, knows when she discovered fraudulent credit card charges, the amount of such charges, and the cost of the credit monitoring services she subsequently purchased. It is likely difficult to reliably obtain such evidence from an independent source without Jane's input. In such cases, one may plausibly conclude that individualized evidence is required to determine the existence and type of loss in question.

Second, significant differences between data breach victims count against the use of representative evidence to displace the need for individualized evidence and to determine damages on a class-wide basis. Briefly stated, using representative evidence to assess damages involves sampling a subset of class members and extrapolating the results to all members.[184] To illustrate with a simple example, suppose that a class action is brought on behalf of 10,000 data breach victims. Suppose further that a survey of a 5%, randomly selected sample of those victims (i.e., 500 victims) reveals that 100 of them suffered a small amount of loss from data misuse ($100 dollars each), ten suffered a large amount ($1,000 each), and the remaining 390 did not suffer any loss. Thus, on average each sample victim suffered a loss of forty dollars (($100 × 100 + $1000 × 10) / 500 = $40). Instead of requiring individualized evidence from class members, the court may simply award each member $40.[185]

There are benefits to using representative evidence to assess damages in this manner. As explained in the next Section, requiring putative class members to adduce individualized evidence to seek damages can be both costly and impractical; it might also prevent many data breach class actions from being brought in the first

182. Support can be found, for example, in appellate decisions that refused to certify a class where the plaintiffs sought relief mainly for emotional distress. *See* Alderwoods Group, Inc. v. Garcia, 119 So. 3d 497, 506 (Fla. Dist. Ct. App. 2013).

183. Researchers have identified relationships between risk of identity theft and various personal characteristics, such as age, gender, income, education, and propensity to take certain security measures. *See* David Burnes, Marguerite DeLiema & Lynn Langton, *Risk and Protective Factors of Identity Theft Victimization in the United States*, 17 PREVENTIVE MED. REPS. 1, 2 (2020).

184. *See* Robert G. Bone, *Tyson Foods and the Future of Statistical Adjudication*, 95 N.C. L. REV. 607, 614–16 (2017).

185. Alternatively, the court may create a subclass of individuals who have incurred loss from data misuse and award each subclass member the average amount of loss incurred by the subset of the sample victims who incurred such loss (i.e., ($100 × 100 + $1000 × 10) / 110 ≈ $181.8).

place.[186] Nevertheless, two objections weigh heavily against using representative evidence to assess damages in the aforementioned manner. The first objection is that this method unavoidably overcompensates some victims and undercompensates others. It seems particularly unfair to individuals who suffered a high amount of loss to be denied the opportunity to prove their loss in court and to receive compensation for only a fraction of the loss suffered.[187] This likely violates the Rules Enabling Act, which forbids interpreting Rule 23 to "abridge, enlarge or modify any substantive right."[188] Indeed, the greater the disparity between victims with respect to their loss, the less accurate the award is in reflecting each victim's actual loss.[189]

The second objection is that although the Supreme Court approved of the use of representative evidence in class actions in *Tyson Foods, Inc. v. Bouaphakeo*,[190] using representative evidence to assess damages for (1) loss from data misuse, (2) mitigation costs, and (3) emotional distress might not be permissible under *Tyson Foods* for two reasons. First, the Court held that the permissibility of a representative or statistical sample turned on "the purpose for which the evidence is being introduced" and "the elements of the underlying cause of action."[191] In *Tyson Foods*, representative evidence was used to overcome an evidentiary difficulty created by the defendant (i.e., its failure to keep records).[192] One plausible reading of *Tyson Foods* is that use of representative evidence should be limited to such cases.[193] If read in this way, then data breach victims cannot rely on *Tyson Foods* to adduce representative evidence to fill evidentiary gaps (e.g., evidence concerning loss from data misuse) which are not created or caused by the defendant. Second, without establishing any general rule, the Court held that it was permissible to use representative evidence to prove class-wide liability if "each class member could have relied on that sample to establish liability if he or she had brought an individual action."[194] However, given the disparities among putative class members, evidence concerning loss suffered by one member has little probative value in proving that another member suffered the same loss. Take mitigation costs as an example. If a class member, Jane, brought an individual action, she cannot prove that she purchased credit monitoring services by adducing evidence that other victims of the same data breach spent an average of $100 on credit monitoring. Jane must

186. For more detailed arguments on the benefits of using representative evidence to adjudicate cases, see Bone, *supra* note 184; Alexandra D. Lahav, *The Case for Trial by Formula*, 90 TEX. L. REV. 571 (2011); Laurens Walker & John Monahan, *Sampling Damages*, 83 IOWA L. REV. 545 (1998).

187. Individuals who have suffered greater loss might choose to opt out of the class action. Nevertheless, this option may not be practical if the amount of loss is not sufficiently great to justify bringing individual proceedings. *See* Bone, *supra* note 184, at 662.

188. 28 U.S.C. § 2072(a)–(b) (2018).

189. For a more detailed analysis of how heterogeneity among class members affects the reliability of sampling methodology, see Bone, *supra* note 184, at 642–49.

190. 577 U.S. 442 (2016). *See also* J. Glover, *The Supreme Court's "Non-Transsubstantive" Class Action*, 165 U. PA. L. REV. 1625 (2017) (arguing that *Tyson Foods* was at odds with both *Comcast Corp. v. Behrend*, 133 S. Ct. 1426 (2013), and *Dukes*).

191. *Tyson Foods*, 577 U.S. at 455 (quoting Erica P. John Fund, Inc. v. Halliburton Co., 563 U.S. 804, 809 (2011)).

192. *Id.* at 442.

193. Bone, *supra* note 184, at 634.

194. *Tyson Foods*, 577 U.S. at 443.

introduce evidence of her own expenditure (e.g., her receipt from a credit monitoring service provider). Therefore, under *Tyson Foods*, putative class members arguably should not be allowed to introduce representative evidence to determine mitigation costs on a class-wide basis. This argument applies with the same force to prevent the use of representative evidence to assess two other types of loss on a class-wide basis: loss from data misuse and emotional distress.

In contrast, the disparities among data breach victims do not necessarily prevent them from arguing that all members of the putative class have suffered a minimum amount of increase in their risk of future harm, and, for that reason, damages can be determined on a class-wide basis.[195] While attractive in theory, this argument is difficult to implement in practice. Firstly, it is difficult to single out the impact of a particular data breach and assess the extent to which that breach leads to an increase in the victim's risk of future injury. Secondly, it is difficult to design a model to assess the minimum amount of increase in risk shared by all members. One possible strategy is to identify the victim who has likely suffered the least amount of increase in risk of harm. However, there is likely little consensus as to the characteristics that victim should possess, such as the person's gender, age, income, education, and online purchasing behavior. Also, it may not be possible to identify that victim without requiring class members to adduce individualized evidence concerning their personal circumstances. Thirdly, even if it is possible to identify the minimal amount of increase in risk of future injury suffered by all victims, the amount may not be sufficiently material to justify legal redress. As noted above,[196] a number of courts are reluctant to find Article III standing based solely on an increased risk of future injury.

b. Bifurcated Proceedings to Assess Damages

Even if individualized evidence is required to determine damages, the court will not necessarily conclude that the predominance requirement is not satisfied and thus decline to certify a class. As the Supreme Court explained in *Tyson Foods*,

> [w]hen one or more of the central issues in the action are common to the class and can be said to predominate, the action may be considered proper under Rule 23(b)(3) even though other important matters will have to be tried separately, such as *damages* or some affirmative defenses peculiar to some individual class members.[197]

One may argue that, in data breach cases, the central issues are clearly common to the class, such as whether the defendant owed the plaintiffs a duty to take data security measures and whether that duty was breached.

---

195. A similar argument was made in a different context in the UK case of *Lloyd v. Google* [2021] UKSC 50, [2022] 2 All ER 209 at [145]–[147] (considering whether every member of the class suffered an "irreducible minimum harm").

196. *See supra* Introduction and note 12.

197. *Tyson Foods*, 577 U.S. at 453–54 (emphasis added) (quoting 7AA CHARLES ALAN WRIGHT, ARTHUR R. MILLER, EDWARD H. COOPER & MARK KAY KANE, FEDERAL PRACTICE AND PROCEDURE 123–24 (3d ed. 2005)).

Therefore, the alternative option is to certify a class action concerning liability, leaving damages assessment to be determined in separate proceedings.[198] However, several related practical difficulties are likely present with this bifurcated process. Firstly, the amount of loss suffered by each individual affected by a data breach is likely too small to incentivize those individuals to bring individualized evidence in a separate proceeding.[199] Many of those individuals may not even be aware of the class action in the first place. This result can be inferred from the fact that, more often than not, only a small proportion of the class members file a claim against the general settlement fund after a data breach action is settled.[200] For instance, of the $1 million settlement fund created by the *In re Heartland* settlement,[201] only $1,925 was paid out to 290 individuals (out of an estimated 130 million potential class members).[202] Secondly, if only a few individuals participate in separate proceedings for damages, the defendant will only be liable for a small amount of damages. This in turn reduces the defendant's incentive to agree to a sizable settlement or to provide adequate data security services in the first place. Moreover, in the absence of the prospect of a large settlement or court order for damages, lawyers (or litigation funders) may not have adequate incentive to pursue a data breach class action to determine liability in the first place. This is particularly the case in the United States where litigants are required to pay their own legal fees;[203] but the same is likely to be true in countries where the losing party pays the other party's legal costs, as the U.K. Supreme Court suggested in the case of *Lloyd v. Google*.[204]

198. *See, e.g.*, Smith v. Triad of Ala., LLC, No. 14-cv-324, 2017 U.S. Dist. LEXIS 38574, at *40–41 (M.D. Ala. Mar. 17, 2017) ("Resolving these claims for damages will require a series of proceedings in which each class member can put on his or her case for damages . . . .").

199. It is questionable whether data breach victims who have suffered a few hundred dollars of loss would find it cost-effective to participate in separate legal proceedings to recover that loss. Let us consider the amount of losses that data breach victims are likely to suffer. Some data breach victims may have suffered identity theft. According to Experian, the median losses per incident for various types of identity theft ranges from $181 to $1,200. *See* Jim Akin, *Identity Theft Statistics: Fraud is on the Rise, Both in Incidents and Losses*, EXPERIAN (Oct. 11, 2022), https://www.experian.com/blogs/ask-experian/identity-theft-statistics/ [https://perma.cc/SZ48-RCMF]. Some victims may have purchased credit monitoring services. While basic credit monitoring is free, premium credit monitoring services can range from $8.99 to $39.95 per month. *See* Alexandria White, *The Best Credit Monitoring Services that can Help You Spot Fraud Early*, CNBC, https://www.cnbc.com/select/best-credit-monitoring-services/ [https://perma.cc/9HMU-H9MU] (Mar. 1, 2023). Some victims may have spent time taking preventive measures. Assuming that $25 is awarded for each hour, a person who has taken 20 hours is entitled to $500. For example, in a settlement involving Experian's data breach, compensation is calculated at $25 per hour. *See In re* Equifax Customer Data Sec. Breach Litig., No. 17-md-2800, 2020 U.S. Dist. LEXIS 118209, at *149 (N.D. Ga. Jan. 13, 2020). Yet, other data breach victims may have experienced stress and anxiety, but have not suffered any financial loss. It is less clear how much loss, if any, they can recover.

200. For a discussion of problems with privacy class actions, see Eric Goldman, *The Irony of Privacy Class Action Litigation*, 10 J. ON TELECOMM. & HIGH TECH. L. 309 (2012).

201. *In re* Heartland Payment Sys., Inc. Customer Sec. Breach Litig., 851 F. Supp. 2d 1040, 1047 & n.2, 1050 (S.D. Tex. 2012).

202. *In re* Hannaford Bros. Customer Data Sec. Breach Litig., 293 F.R.D. 21, 26 (D. Me. 2013).

203. This problem may be alleviated by enacting statutory provisions to allow the court to order the defendant to pay for data breach class actions. For a brief explanation of fee-shifting statutes, see RICHARD A. NAGAREDA, ROBERT G. BONE, ELIZABETH CHAMBLEE BURCH & PATRICK WOOLEY, THE LAW OF CLASS ACTIONS AND OTHER AGGREGATE LITIGATION 391–92 (3d ed. 2020).

204. Lloyd v. Google [2021] UKSC 50, [2022] 2 All ER 209 at [85].

c. Unjust Enrichment: Determine Remedy on a Class-Wide Basis

In contrast, it is likely that the amount of restitution for overpayment for data security can be determined on a class-wide basis. To begin with, all putative class members rely on a unifying theory of recovery—the defendant received payment for providing reasonable data security but did not do so. It is likely unnecessary for each member to introduce individualized evidence to prove that he or she is entitled to seek restitution based on this theory: all putative class members would have purchased similar types of goods or services (e.g., insurance policies) from the same defendant under substantially similar terms.[205] The defendant therefore likely possesses written records of these purchases and the terms based on which those purchases were made. The question of whether the plaintiffs have indeed paid for data security services can be determined by examining those terms in light of the circumstances. The answer is unlikely to turn on each class member's personal characteristics, such as income and education.

Similarly, individualized evidence is unlikely to be necessary to determine the amount recoverable based on the overpayment theory. As argued above, in the absence of express agreement, the amount recoverable should be assessed by an objective standard—the reasonable price for the defendant to charge and the class members to pay for data security.[206] While the reasonable price of data security may be determined by factors such as the type of personal data transferred and the cost of providing adequate data security, these factors can generally be ascertained without requiring individualized evidence from each class member.[207] Moreover, the reasonable price of data security may be expressed as a percentage of the price of the goods and services purchased to take account of the fact that each class member may have spent varying amounts on those goods and services.

Further, putative class members may wish to rely on representative evidence to establish the reasonable price for data security. For example, they may wish to introduce survey or experimental evidence showing that the putative class members, or other individuals, are likely willing to pay a certain sum for data security. Using representative evidence for this purpose is much less objectionable for several reasons. Firstly, such evidence likely has probative value in determining the reasonable value, if any, of the relevant data security services. More importantly, the evidence does not determine the value of those services, it is merely one factor that the court takes into account in deciding the reasonable price of data security. Secondly, relying on representative evidence for this purpose is likely permissible under *Tyson Foods*: even if Jane brought an individual unjust enrichment action, she should still be allowed to adduce such evidence to demonstrate that (1) data security services likely have a measurable value; and that (2) it is reasonable for her to place a similar value on the services in question, provided that the relevant study satisfies the test for admissibility of scientific evidence in *Daubert v. Merrell Dow*

205. Many businesses use standard form contracts when they enter into transactions with their customers.

206. *See supra* Section I.A.2.a.ii.

207. For example, expert evidence may be obtained to assist in determining the cost of providing certain types of data security measures.

Pharmaceutical.[208] At the end of the day, whether representative evidence should be allowed for the purpose of establishing remedies in data breach cases likely turns on policy considerations. Given that most data breach victims suffer a small amount of loss, the alternative to a class action is not multiple individual actions, but no action at all. The court is likely more willing to allow plaintiffs to rely on representative evidence to enable class actions to be brought against companies that fail to provide adequate data security for deterrence purposes.[209] An unjust enrichment claim based on overpayment for data security allows the court to do so without significant departure from existing authorities.

Moreover, where plaintiffs seek to recover the use value of their personal data based on the "would not have shopped" theory, the total amount of use value recoverable depends on how the data is used by the defendant and thus can be determined without individualized evidence from the plaintiffs. While each class member may have transferred different amounts of personal data to the defendant, the defendant is likely to have a record of such information, making it unnecessary for each class member to adduce individualized evidence. In any event, it is arguably appropriate for class members to recover the same amount of use value for their data in many cases because (1) their data is of little value except as part of a database; and (2) it is generally not cost-effective to ascertain the exact amount of data transferred by each member.

2. Individualized Evidence to Establish Causation

Secondly, defendants may argue that the predominance requirement is not satisfied because individualized evidence is required to establish that each putative class member suffered loss as a result of the defendant's failure to secure their data.

a. The Need for Individualized Evidence to Recover Consequential Loss

If data breach victims bring tort or contract claims to recover (1) loss from data misuse, (2) mitigation costs, (3) emotional distress, or (4) increased risk of future injury, they must establish a *causal* link between their loss and the defendant's breach.[210] Both the Ninth and Eleventh Circuits noted that a causal link cannot be established by showing a mere "temporal connection"[211] between a data breach and the plaintiffs' loss: for example, the mere fact that a plaintiff suffered identity theft six weeks after a data breach is not sufficient in and of itself to prove causation.[212] Nevertheless, the Eleventh Circuit accepted in *Resnick* that causation can be established through circumstantial evidence, provided that the evidence shows "a nexus between the two instances beyond allegations of time and sequence."[213]

---

208. Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993). *Daubert* requires the court to determine "whether the reasoning or methodology underlying the testimony is scientifically valid and . . . whether that reasoning or methodology properly can be applied to the facts at issue." *Id.* at 592–93.

209. *See, e.g.*, NAGAREDA, BONE, BURCH & WOOLEY, *supra* note 203, at 636 (suggesting that the purpose of sampling is to "secure the statute's compensation and deterrence goals").

210. *See, e.g.*, Stollenwerk v. Tri-West Health Care All., 254 F. App'x 664, 668 (9th Cir. 2007).

211. *Id.* at 668, *cited with approval in* Resnick v. AvMed, Inc., 693 F.3d 1317, 1327 (11th Cir. 2012).

212. *Id.* at 667–68.

213. *Resnick*, 693 F.3d at 1326–28.

However, such circumstantial evidence often requires class members to provide individualized evidence, such as their data disclosure histories as well as incidents of prior identity theft.[214]

The difficulty of establishing causation on a class-wide basis is one plausible ground for concluding that the predominance requirement is not satisfied.[215] Alternatively, the court may adopt a bifurcated approach: it can certify a class for specific issues, but leave causation to be determined in a series of proceedings in which class members are required to adduce individualized evidence.[216] One of the problems with this bifurcated approach, as explained more fully in the last Section, is that a large percentage of the data breach victims may not be sufficiently incentivized to adduce evidence in those separate proceedings, which in turn significantly reduces the potential liability for the defendant.

b. Causation in Unjust Enrichment Claims

In contrast, in an unjust enrichment claim based on overpayment for data security, once the plaintiffs establish that the defendant received remuneration for adequate data security but did not provide it, the plaintiffs should be entitled to recover the overpaid sums.[217] As the majority in *Resnick* put it, "Plaintiffs' unjust enrichment claim does not have a causation element."[218] Consequently, a defendant cannot seek to defeat class certification based on the need for individualized evidence to establish causation.

By contrast, an unjust enrichment claim based on the "would not have shopped" theory *prima facie* requires class members to introduce individualized evidence to show that they would not have purchased products or services had they known about the defendant's inadequate data security. As such, there is a higher chance that the court might refuse to certify a class on the basis that the predominance requirement is not satisfied. Nevertheless, a possible argument is that such individualized evidence may not be necessary if it can be shown (1) that the relevant use is prohibited by the contract or (2) that data security is so indispensable to the transaction in question that no reasonable plaintiff would have entered into the transaction without adequate data security.

3. Individualized Defense

Thirdly, defendants may argue that the predominance requirement is not satisfied because they intend to litigate defenses to individual claims.

---

214. *See, e.g.*, *Stollenwerk*, 254 F. App'x at 668 (holding a reasonable jury could find a causal relationship based on the plaintiff's allegations, including that "(1) he does not transmit personal information over the internet, (2) he shreds mail containing personal information, and (3) the only other known incident of his personal information being stolen [occurred at least five years ago].").

215. *See, e.g.*, *In re* TJX Cos. Retail Sec. Breach Litig., 246 F.R.D. 389, 397 (D. Mass. 2007) (concluding that one of the reasons why the predominance requirement was not satisfied was because causation could not be established on a class-wide basis).

216. *See, e.g.*, Smith v. Triad of Ala. LLC, No. 14-cv-324, 2017 U.S. Dist. LEXIS 38574, at *42 (M.D. Ala. Mar. 17, 2017).

217. *See supra* Section I.A.2.c.

218. *Resnick*, 693 F.3d at 1328.

a. The Need for Individualized Evidence

In *Dukes*, the Supreme Court held that "[b]ecause the Rules Enabling Act forbids interpreting Rule 23 to 'abridge, enlarge or modify any substantive right,' a class cannot be certified on the premise that Wal-Mart will not be entitled to litigate its statutory defenses to individual claims."[219] Relying on *Dukes*, defendants in data breach class actions might argue that allowing putative class members to use representative evidence to determine damages relating to (1) loss from data misuse, (2) mitigation costs, or (3) emotional distress on a class-wide basis would prevent the defendant from litigating its defenses—such as contributory negligence—to individual claims, which violates the Rules Enabling Act. It is conceivable that some data breach victims might suffer loss partially due to their own negligence. For example, suppose that John's email was disclosed in a data breach. Suppose further that John subsequently suffered financial loss after clicking on a link in a phishing email. John may be considered contributorily negligent for that loss if no reasonable person would have clicked on that link.

b. Unjust Enrichment: Defendant-sided Defense

In contrast, one of the most important defenses to unjust enrichment claims is change of position.[220] Assuming that this defense applies to unjust enrichment claims for overpayment of data security,[221] the defense focuses on the defendant's conduct to determine whether restitution is inequitable to the defendant.[222] Consequently, the defendant can raise this defense without individualized evidence from putative class members.

c. Little Risk of Overdeterrence

Lastly, as commentators have noted, courts often refuse to certify a class action consisting of all affected consumers, "opting instead to certify subclasses whose involvement can be verified more precisely."[223] For example, in *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*,[224] in light of the Maine Supreme Judicial Court's refusal to recognize lost time and effort as a cognizable injury, the plaintiffs had to recast their putative class to include only individuals who made "out-of-pocket expenditures . . . in reasonable attempts to mitigate against economic injury" from the data breach.[225] Similarly, in *In re Brinker Data Incident*

219. Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 367 (2011).

220. Other defenses are arguably less relevant in the overpayment for data security context. For example, recovery in restitution may be limited or denied due to the plaintiff's "inequitable conduct in the transaction that is the source of the asserted liability." RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 63 (AM. L. INST. 2011). This defense is more commonly raised in situations in which plaintiffs seek restitution for "benefits conferred under a contract that is illegal or unenforceable for reasons of public policy." *Id.* at cmt. b.

221. This defense is clearly available against unjust enrichment claims based on invalidating mistake.

222. *See* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT (2011) § 65 (AM. L. INST. 2011).

223. *See, e.g.*, Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 563 (2016).

224. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 293 F.R.D. 21 (D. Me., 2013).

225. *Id.* at 24.

Litigation, the court narrowed the putative class definition to include only those individuals who have had their data "accessed by cybercriminals" and those that have "incurred reasonable expenses or time spent in mitigation of the consequences of the [d]ata [b]reach" [226] to avoid potential challenges to class members' standing. A possible consequence of certifying only a subclass of victims is that the defendant may not fully internalize the negative externalities created by its failure to take reasonable data security measures.

By contrast, an unjust enrichment claim based on overpayment should allow all data breach victims to seek recovery against the defendant, provided that the latter has received payment for data security services, but failed to provide them.[227] A data breach can sometimes involve millions of individuals. Even assuming that the value of adequate data security in a particular case is only one dollar, the relevant defendant can potentially be liable for millions of dollars (excluding legal fees) each time it suffers a data breach. This amount is higher than the amount of settlement reached in many privacy class actions to date.[228]

An argument can be made that an unjust enrichment claim based on overpayment makes the cost of a data breach too high—a single data breach can be financially devastating for some companies. Such a result is out of proportion to the actual harm suffered by victims of the data breach since many of them may not have suffered or ever will suffer any significant financial loss as a result of that data breach. In other words, more prevalent use of unjust enrichment as a cause of action in data breach cases might result in overdeterrence. As the Second Circuit has acknowledged, in a class action, "the potential for a devastatingly large damages award, out of all reasonable proportion to the actual harm suffered by members of the plaintiff class, may raise due process issues."[229]

However, this overdeterrence problem may not be as serious as it appears at first sight. It is submitted that an unjust enrichment claim based on overpayment arguably strikes a proper balance between providing credible deterrence against irresponsible data practices and excessively interfering with ordinary business. Firstly, as mentioned above,[230] in the absence of an express promise to provide a higher level of data security, a defendant should only be required to take reasonable security measures in accordance with industry standards. Also, the mere fact that a defendant has suffered one or multiple data breaches does not in and of itself prove that the defendant failed to provide adequate data security. In fact, the defendant can always introduce evidence to demonstrate that it has acted in accordance with prevailing industry standards. Secondly, while an award for damages can be unexpectedly high depending on how data is actually misused and the plaintiffs' personal circumstances (e.g., in the case of loss from medical identity theft), the total amount that a defendant can be liable for in an unjust enrichment claim is both

---

226. *In re* Brinker Data Incident Litig., No. 18-cv-686, 2021 U.S. Dist. LEXIS 71965, at *20 (M.D. Fla. Apr. 14, 2021).

227. Strahilevitz also pointed out that unjust enrichment has the effect of increasing the class size in data breach class actions. *See* Strahilevitz, *supra* note 20, at 2489.

228. *See* Katherine Cienkus, *Privacy Class Action Settlement Trends: Industry Practice or Improper Incentives?*, 40 REV. OF LITIG., Spring 2021, at 40–46.

229. Parker v. Time Warner Ent. Co., 331 F.3d 13, 22 (2d Cir. 2003).

230. *See supra* Section I.A.2.a.ii.

predictable and limited—it is a portion of the payment made by the plaintiffs to the defendant in the first place. Therefore, a defendant can adjust the price of its products or services in light of the actual cost of data security. Related to this, one might argue that more prevalent use of the unjust enrichment claim might result in an increase in price for goods and services. However, this may not necessarily be a bad thing if it means that database holders are finally taking reasonable data security measures. The increase in price may be justified by the decrease in the various types of financial and non-financial losses which can result from irresponsible data handling.[231] This price increase might also serve a useful loss distribution function similar to that of an insurance.[232]

III. CONTRACTUAL LIMITS ON UNJUST ENRICHMENT CLAIMS

Nevertheless, the effectiveness of unjust enrichment in deterring irresponsible data practice should not be overstated. This Section considers two contract-related grounds for defeating such claims.

A. Preemption by Contract

First, a number of both majority and dissenting opinions in federal courts have concluded that data breach victims could not bring an unjust enrichment claim because there was a contract between the parties concerning the same subject matter (the "preemption rule").[233] Some courts held that the existence of a valid contract alone precludes a claim for unjust enrichment."[234] Other courts took a more defensible approach.[235] For example, in *Kuhns*, the Privacy Statement in Kuhn's

231. See *supra* Section I.A.3.b for the various types of losses that a data breach victim might suffer.

232. *See* Moin A. Yahya, *Can I Sue Without Being Injured: Why the Benefit of the Bargain Theory for Product Liability is Bad Law and Bad Economics*, 3 GEO. J.L. & PUB. POL'Y 83, 83 (2005) (claiming that the price of products generally includes "an insurance premium that the manufacturer collects to compensate consumers").

233. Resnick v. AvMed, Inc., 693 F.3d 1317, 1332 (Pryor, J., dissenting) (first citing Diamond "S" Dev. Corp. v. Mercantile Bank, 989 So. 2d 696, 697 (Fla. Dist. Ct. App. 2008); then citing Am. Safety Ins. Serv., Inc. v. Griggs, 959 So. 2d 322, 331 (Fla. Dist. Ct. App. 2007)); *In re* Zappos.com, Inc. Customer Data Sec. Breach Litig., No. 12-cv-00325, 2016 U.S. Dist. LEXIS 60453, at *24 (D. Neb. May 6, 2016) (dismissing plaintiffs' unjust enrichment claim because "they failed to allege that they conferred any benefit upon Zappos outside of the contracts they formed to purchase goods"); Attias v. CareFirst, Inc. 365 F. Supp. 3d 1 (D.D.C. 2019); Bovay v. Sears, Roebuck & Co., No. 1-14-2671, 2017 Ill. App. Unpub. LEXIS 35, at *80 (Ill. App. Ct. 2017) ("Furthermore, the unjust enrichment claims fail because the relationship between Sears and plaintiffs was governed by the agreements during the class period . . . Given the various agreements that governed the relationships between Sears and plaintiffs during the class period, plaintiffs' 'quasi-contract' unjust enrichment claims fail.").

234. *See, e.g.*, *Attias*, 365 F. Supp. 3d at 25; *Bovay*, 2017 Ill. App. Unpub. LEXIS 35, at *80. The same observation was made in Chao, *supra* note 3, at 587–88.

235. *See, e.g.*, Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. 2017); *In re* Sony Gaming Networks, 996 F. Supp. 2d 942, 984 (S.D. Cal. 2014) ("Under Florida, Massachusetts, Michigan, Missouri, New Hampshire, New York, Ohio, and Texas law a plaintiff may not recover for unjust enrichment where a 'valid, express contract governing the subject matter of the dispute exists' (Coghlan v. Wellcraft Marine Corp., 240 F.3d 449, 454 (5th Cir. 2001) (applying Texas law)). Here, neither party contests the validity of the PSN/SOE User Agreements and the PSN/SOE Privacy Policies, and Plaintiffs rely on these exact agreements to support their allegations. Therefore, because Plaintiffs do not argue that the agreements are somehow invalid or otherwise unenforceable, Plaintiffs are not permitted to plead unjust enrichment as an alternative to breach of contract claims.").

Brokerage Agreements with Scottrade represented that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings," and "Scottrade provides Secure Socket Layer encryption."[236] According to the Eighth Circuit, the fact that the Brokerage Agreement "covered the subject of customer data security" was sufficient to prevent Kuhns from bringing an unjust enrichment claim based on overpayment for data security.[237]

Assuming that the security representations in *Kuhns* are contractually enforceable promises, the court's application of the preemption rule appears to reflect the prevailing academic view.[238] Section 2 of the *Restatement* states the general principle: "[a] valid contract defines the obligations of the parties as to matters within its scope, displacing to that extent any inquiry into unjust enrichment."[239] Dobbs' Law of Remedies also maintains that unjust enrichment is "not the proper avenue for relief" for partial breach of contract because "contract remedies should govern enforceable contracts."[240] The main justification for the preemption rule is that contract law is a more effective means than unjust enrichment to regulate voluntary transfers.[241] The court should respect the intention of the parties and give effect to their own valuation of benefits and allocation of risks, as expressed in their contract.[242] It should not allow a party to escape a bad bargain by pursing an alternative unjust enrichment claim.[243]

If the justification of the preemption rule is to respect the parties' intentions and their contractual allocation of risk, then it follows that, even if there is a valid and subsisting contract governing the same subject matter (e.g., data security), unjust enrichment claims should be permitted if they do not undermine the contractual allocation of risk.[244] In other words, if data breach victims prefer to bring an unjust enrichment claim instead of a breach of contract claim, they should be allowed to do so.[245]

Where the relevant contract does not specify the remedy for failing to comply with data security obligations, there is arguably a gap in the contractual allocation of risk. The unjust enrichment principles proposed in this Article help fill that gap.

---

236. *Kuhns*, 868 F.3d at 717.

237. *Id.* at 718.

238. *See, e.g.*, RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 2 (AM L. INST. 2011); DAN B. DOBBS & CAPRICE L. ROBERTS, LAW OF REMEDIES: DAMAGES, EQUITY, RESTITUTION § 12.7(1) (3d ed. Supp. 2017); Andrew Kull, *Disgorgement for Breach, the "Restitution Interest," and the Restatement of Contracts*, 79 TEX. L. REV. 2021, 2022, 2041–42 (2001).

239. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 2(2) (AM. L. INST. 2011).

240. DAN B. DOBBS & CAPRICE L. ROBERTS, LAW OF REMEDIES: DAMAGES, EQUITY, RESTITUTION § 12.7(1) (3d ed. 2017).

241. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 2(2) cmt. c (AM. L. INST. 2011).

242. *Id.*

243. Stephen Smith, *Concurrent Liability in Contract and Unjust Enrichment: The Fundamental Breach Requirement*, 115 LAW Q. REV. 245, 245–46 (1999).

244. This point was also made in GOFF & JONES: THE LAW OF UNJUST ENRICHMENT § 3–17 (Charles Mitchell, Paul Mitchell & Stephen Watterson eds., 9th edition ed. 2016).

245. *Id.* (citing Jack Beatson, *Restitution and Contract: Non-Cumul?* 1 THEORETICAL INQ. L., Jan. 2000, at 83).

The author does not suggest that this is the only way to fill the gap, but the mere fact that the gap can be filled in other ways (e.g., by inserting an implied term to a contract between the parties) should not by itself preclude the application of unjust enrichment law.

In fact, data breach victims might prefer to invoke unjust enrichment principles for various reasons. First, an unjust enrichment claim might be considered more intuitive or easier to assert, particularly where the plaintiffs have paid a premium for data security. To illustrate this point, assume that a specific portion of the payment is expressly allocated for data security ($10) and that the amount is higher than the market value of the relevant data security services (which is valued at $8). If the defendant fails to take any data security measure, then the plaintiffs should be entitled to recover the overpayment in full (i.e., $10) in an unjust enrichment claim.[246] By contrast, in a breach of contract claim, the plaintiffs might have to further explain why their recovery should not be capped by the market value of the services that they bargained for (i.e., $8).[247] Second, in appropriate cases, plaintiffs might also prefer to bring unjust enrichment claims for procedural or evidentiary reasons (e.g., more favorable limitation period).[248] Third, unjust enrichment, as a distinct cause of action, does not necessarily require proof of breach of contract or tortious/criminal conduct.[249] Where the relevant contract is a standard form contract, allowing the plaintiffs to pursue more avenues of redress might have the additional benefit of avoiding tilting the balance of power too far towards companies who are often in a position to dictate the terms of the contract.

In light of the above, arguably data breach victims should be allowed to pursue unjust enrichment claims even if there is a valid and subsisting contract governing data security provided that their unjust enrichment claims do not undermine the contractual allocation of risk.[250]

Finally, it is worth noting that, even if a court reaches a contrary conclusion and the plaintiffs are barred from pursuing unjust enrichment claims, the plaintiffs might nevertheless be able to disgorge profits (in the form of saved expenditure)

---

246. *See supra* Section I.A.2.

247. In contract law, expectation damages aim to put the plaintiff "in as good a position as he would have been in had the contract been fully performed, and no better." *See* DAN B. DOBBS & CAPRICE L. ROBERTS, LAW OF REMEDIES: DAMAGES, EQUITY, RESTITUTION § 12.2(1) (3d ed. 2017). In this scenario, had the contract been fully performed, the plaintiffs would have received services worth $8. Allowing the plaintiffs to recover $10 appears to put them in a better position and hence arguably results in overcompensation. Nevertheless, an argument can be made that allowing the plaintiffs to recover $10 is not inconsistent with contract law principles. For example, Andrew Kull argues that "[r]estitution of a prepaid purchase price, without reference to the market value of a performance that the defendant has failed to render, is justified by the equity, the simplicity, and the efficiency of the remedy in such circumstances." *See* Kull, *supra* note 238, at 2022, 2041–42 (2001). In contrast, plaintiffs do not have to resort to such argument when bringing an unjust enrichment claim to recover $10.

248. This point was made in Beatson, *supra* note 245. The limitation period for unjust enrichment claims is determined by local law. For more details, see RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 70 (AM. L. INST. 2011).

249. *See supra* Section I.A.4. "Liability in restitution is often independent of fault." *See* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 cmt. f (AM. L. INST. 2011).

250. In England, several academics have also argued in favor of allowing concurrent claims in contract and unjust enrichment. *See, e.g.*, Smith, *supra* note 243; Andrew Tettenborn, *Subsisting Contracts and Failure of Consideration - A Little Scepticism*, 10 RESTITUTION L. REV. 1 (2002).

retained by the defendant as a result of its deliberate breach of the contractual promise to secure data.[251] Under existing law, disgorgement for breach of contract is only allowed in very limited circumstances.[252]

B. Easy to Contract out of Liability

Secondly, the availability of an unjust enrichment claim can be excluded by an express term in the contract. For example, in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, the plaintiffs' unjust enrichment claim was dismissed because Sony clearly stated in its privacy policy that it "[could] not ensure or warrant the security of any information transmitted to [Sony]."[253] In other words, to preempt an unjust enrichment claim, database holders can simply insert similar exemption clauses in their contracts. In practice, it is unlikely that consumers will read these exemption clauses.[254]

Nevertheless, it is questionable whether the availability of an unjust enrichment claim will invariably cause database holders to include onerous exemption clauses in their contracts.[255] Firstly, consumers may have higher expectations for data security from companies that provide certain types of products or services, such as cellphones and insurance. Therefore, it may not be in the company's best financial interest to include such disclaimers in their contracts. In fact, some companies might even prefer to compete on data security. For example, Apple has positioned itself as a privacy-sensitive technology company: it famously contested a court order to help the Federal Bureau of Investigation circumvent security software by unlocking an iPhone belonging to a shooter.[256] Secondly, depending on state laws on exemptions clauses and unfair contract terms,

---

251. For a more detailed analysis of disgorgement of profits in this context, see Chao, *supra* note 3, at 584–87.

252. According to § 39 of the RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT (AM. L. INST. 2011), plaintiffs are entitled to seek disgorgement of profits for breach of contract provided that several conditions are satisfied. First, the defendant must have committed a "deliberate breach." What type of conduct amounts to a "deliberate breach" is far from clear. But mere proof that the defendant negligently failed to provide adequate data security is likely insufficient in light of the Supreme Court decision in *Kansas v. Nebraska*, 574 U.S. 445 (2014). Moreover, the plaintiff must show that "the available damage remedy affords inadequate protection." As the authors of the *Restatement* have acknowledged, "a breach of contract that satisfies the cumulative tests of § 39 is rare." RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 39, cmt. a (AM. L. INST. 2011).

253. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 981 (S.D. Cal. 2014).

254. According to one study, if an American online user were to read the privacy policies for every site she visited, she would likely spend 244 hours a year (40 minutes per day) reading privacy policies. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J OF L & POL'Y FOR INFO. SOC'Y 543, 563 (2008)*; see also*, Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 546 (2014) ("Consumers seldom read the form contracts that firms offer.").

255. Even if some companies choose to include onerous exemption clauses, this might have some desirous effect. It might serve as a signal that those companies are less privacy-protective.

256. Chris Fox & Dave Lee, *Apple Rejects Order to Unlock Gunman's Phone*, BBC NEWS (Feb. 17, 2016), https://www.bbc.com/news/technology-35594245 [https://perma.cc/8P93-CGWQ].

database holders may not be able to exclude liability for gross negligence or sometimes even negligence.[257]

IV. RESTITUTION FOR NEGLIGENT FAILURE TO SECURE DATA

This Part discusses several situations in which the plaintiffs may be entitled to seek restitution as a remedy for the defendant's failure to comply with common law or statutory obligations to secure the plaintiffs' personal data.

As noted at the beginning of this Article,[258] a company that collects and retains the plaintiffs' personal data may not necessarily owe a duty to secure that data. While some courts recognize a duty to take reasonable precautions in such situations,[259] a number of appellate courts take the view that there is no general duty to safeguard personal data.[260] Moreover, some courts maintain that a defendant's duty to safeguard personal data arises from its knowledge of a foreseeable risk to its data security systems.[261] This suggests that defendants without such knowledge might not owe such a duty. Further, there is no general duty to protect someone from criminal attacks by third parties.[262] Therefore, where a data breach is caused by hackers, plaintiffs must overcome additional hurdles to persuade the court that the defendant owes a duty to protect them from criminal conduct due to special circumstances.[263] Additionally, plaintiffs have had mixed success in bringing negligence per se claims based on alleged violations of privacy and consumer protection statutes, such as the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA)[264] and the Federal Trade Commission Act (FTC Act).[265]

---

257. Chao raised similar arguments in Chao, *supra* note 3, at 603.

258. *See supra* Introduction.

259. *See, e.g.*, *In re* Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 514, 529 (M.D. Pa. 2021); *In re* Am. Med. Collection Agency Customer Data Sec. Breach Litig., No. 19-md-2904, 2021 U.S. Dist. LEXIS 240360, at *57–59 (D.N.J. Dec. 16, 2021); Brush v. Mia. Beach Healthcare Grp. Ltd., 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014); Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898, 915 (S.D. Cal. 2020).

260. *See, e.g.*, McConnell v. Dep't of Lab., 814 S.E.2d 790, 799 (Ga. Ct. App., 2018) (concluding there is no duty of care to safeguard personal information under Georgia law); Cooney v. Chi. Pub. Schs., 943 N.E.2d 23, 28–29 (Ill. App. Ct., 2010). District court decisions refusing to recognize a duty to safeguard the plaintiffs' personal data include *Irwin v. Jimmy John's Enter., LLC*, 175 F. Supp. 3d 1064, 1071 (C.D. Ill. Mar. 29, 2016).

261. *See, e.g.*, *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1325 (N.D. Ga. 2019).

262. *See, e.g.*, Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477 (D.C. Cir. 1970).

263. *See, e.g.*, *In re* Blackbaud, Inc., Customer Data Breach Litig., 567 F. Supp. 3d 667, 682 (D.S.C. 2021) (finding the existence of special circumstances based on the defendant's contractual duties and its negligence "in creating the risk by failing to use reasonable security measures").

264. *See, e.g.*, *id.* at 683–84 (holding that plaintiffs could not base negligence per se claims on HIPAA).

265. Some courts have allowed a negligence per se claim based on violations of the FTC Act to go forward at the motion to dismiss stage. *See, e.g.*, *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 481–82 (D. Md. 2020) (holding plaintiffs adequately pled negligence per se under Georgia law); *In re* Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 406–08 (E.D. Va. 2020) (holding a negligence per se claim could be premised on the FTC Act under New York law). Other courts have refused to allow such claims. *See, e.g.*, *In re* Sonic Corp. Customer Data Sec. Breach Litig., No. 17-md-2807, 2020 U.S. Dist. LEXIS 114891, at *6 (N.D. Ohio July 1, 2020).

Not surprisingly, commentators have argued in favor of recognizing a duty for database holders to secure the personal data in their possession.[266] For example, Lichtman and Posner argue in favor of imposing liability on internet service providers to prevent cyberattacks.[267] Meiring de Villiers suggests that database owners should be liable for failing to patch certain computer security vulnerabilities where their failure foreseeably encourages "free radicals" to commit torts or crimes.[268] Jack Balkin argues that certain digital media companies should be classified as "information fiduciaries" and owe three basic duties towards their users, including a duty to secure the personal data in their possession.[269]

Assume that data breach victims can establish that the defendant owes them a common law duty to protect their personal data and that the duty is breached. Assume further that the defendant has saved non-negligible costs as a result of that breach. For example, the defendant may have saved costs by failing to encrypt sensitive data stored in its devices, failing to patch well-known software vulnerabilities, or failing to implement internal compliance programs that aim at detecting and mitigating security risks. Data breach victims may then argue that the defendant is unjustly enriched by the amount of costs saved. As the *Restatement* explains, enrichment may take any form, including a "saved expenditure."[270] Section 44 of the *Restatement* further states that "[a] person who obtains a benefit by conscious interference with a claimant's legally protected interests . . . is liable in restitution as necessary to prevent unjust enrichment."[271] Conscious interference might be found in situations in which a company knowingly chooses to take data security measures that fall below the standard that can be reasonably expected from such a company. Data breach victims may in turn argue that it is unjust for the company to benefit from a failure to comply with its common law duty and that restitution is necessary to prevent such unjust enrichment. The need for restitution as a remedy is compounded by the fact that, under existing law, it is often very difficult for data breach victims to obtain compensation for loss suffered as a result of inadequate data security.[272]

In a similar vein, if data breach victims succeed in establishing that the defendant has saved costs by consciously choosing not to comply with data security obligations imposed by any legislation, the victims might rely on Section 44 of the *Restatement* to seek restitution of the costs saved on the basis that the defendant is unjustly enriched.[273] However, a violation of statute or regulation per se does not necessarily entail that the defendant is *unjustly* enriched.[274] The *Restatement* provides

266. *See supra* Introduction and note 14.

267. Lichtman & Posner, *supra* note 14, at 222–23.

268. de Villiers, *supra* note 14.

269. *The Fiduciary Model of Privacy*, *supra* note 14.

270. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 cmt. d (AM. L. INST. 2011).

271. *Id.* § 44(1).

272. *See supra* Introduction and Part II.

273. For an overview of federal statutes and regulations that impose data security obligations, see Chapter 2 of PHILIP N. YANNELLA, CYBER LITIGATION: DATA BREACH, DATA PRIVACY & DIGITAL RIGHTS 27–52 (2021 ed.).

274. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 44, reporter's note to cmt. d (AM. L. INST. 2011).

that restitution may be denied "if allowance of the claim would conflict with liabilities or penalties for the interference provided by other law."[275] As such, restitution might be denied (a) if the relevant legislation does not provide a private cause of action (e.g., FTC Act and HIPAA) or (b) if the relevant legislation requires proof that the plaintiff has suffered injury, which the plaintiff fails to establish.[276]

Moreover, Section 43 of the *Restatement* provides that "[a] person who obtains a benefit (a) in breach of a fiduciary duty, [or] (b) in breach of an equivalent duty imposed by a relation of trust and confidence . . . , is liable in restitution to the person to whom the duty is owed." If certain database holders are eventually recognized as "information fiduciaries," data breach victims might be able to rely on this Section to recover any costs saved by those database holders by failing to take reasonable measures to secure the personal data in their possession.[277]

Some of the main difficulties in these claims lie in proving that the defendant has indeed saved costs by failing to provide adequate data security and, if successful, in assessing the amount of said savings. The court might be required to determine both (a) the amount that a company *should* have spent to comply with its often multifaceted data security obligations and (b) the amount that the company has *actually* spent on data security. It would not be easy to make such assessments.[278] Even if the court manages to quantify the saved expenditure, the court must proceed to undertake the difficult task of determining the number of individuals who are entitled to recover those expenses and the amount that each plaintiff can recover. Further, the defendant might not have saved any expenditure. For example, it might have incurred significant costs in providing data security services which turn out to be defective. In such cases, it appears more appropriate for the plaintiffs to rely on the overpayment or "would not have shopped" theory of unjust enrichment as proposed in this Article.

CONCLUSION

This Article provides two main contributions to the existing literature on unjust enrichment claims in data breach and other privacy cases. First, the Article critically analyzes the two main theories of unjust enrichment observed in data breach cases: the overpayment theory and the "would not have shopped" theory. It in turn proposes an alternative, and more plausible, account of the elements that

275. *Id.* § 44(3)(d).

276. *See id.* § 44, reporter's note to cmt. d. ("'To permit plaintiffs to pursue their claim under the label 'unjust enrichment' would allow them to circumvent the law and public policy reflected in (1) [the statutory] mandate that only an injured plaintiff may assert a privacy action under [the consumer protection statute], and (2) the Legislature's decision not to create a private right of action for violations of the Insurances Code sections relevant to this case.") (citing Peterson v. Cellco P'ship, 164 Cal. App. 4th 1583 (2008)).

277. Note, however, that some scholars question the information fiduciary framework. *See, e.g.*, Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019). Moreover, even if certain companies are properly viewed as information fiduciaries, their duty to secure personal data may not necessarily be a fiduciary duty. Therefore, data breach victims might not be able to rely on Section 43 to seek restitution on the basis that there has been a breach of fiduciary duty.

278. As Chao points out, it may be unclear how much money a company wrongfully saved by failing to adopt a compliant program. *See* Bernard Chao, *Unjust Enrichment: Standing Up for Privacy Rights*, 108 IOWA L. REV. ONLINE 49.

must be proved for the overpayment theory. Second, it explains how the facilitative effects of these unjust enrichment claims on class actions solve a powerful enforcement deficit with respect to data security.