A Fiduciary Judge's Guide To Improving Outcomes for Victims in Federal Data Breach Class Actions

Tomasso Piccirilli*

TABLE OF CONTENTS

* J.D., May 2024 , The George Washington University Law School; B.A. December, 2019, History and Economics, American University Honors Program. I would like to thank the entire FCLJ editorial team for their support and feedback. I would especially like to thank Adam Schulman, without whom I would never have discovered class action law.

I. INTRODUCTION

We have all left our phones unlocked, clicked on phony links, or used bad passwords. Even if you practiced perfect data security, the fact of the matter is that data breaches have become an inevitable part of online life, and at least some of your personal data is out there on the dark web, waiting to be used by criminals. Still, you would hope that major corporations would at least try to protect your data. Instead, for many companies, an audit of their data security records reveals astonishing histories of negligence, and consumers can do very little about it.

Take Facebook for instance.[1] In 2018, it was revealed that Facebook's refusal to implement its own security policies resulted in the sale of over eighty-seven million users' data through the political consulting firm Cambridge Analytica.[2] That same year, the New York Times discovered Facebook had been sharing user data with third parties without users' permission.[3] In 2019, three separate databases were found on the dark web containing the Personally Identifiable Information (PII) of between 200 and 540 million Facebook users.[4] Later that year, privacy watcher KrebsOnSecurity revealed that Facebook had stored the passwords of between 200 and 600 million users in unencrypted plaintext.[5] In June of 2020, Facebook disclosed an issue that enabled third-party app developers to access the personal data of users' friends, including emails, names, and hometowns, without their consent.[6] Finally, in 2021, PII for users in 106 countries was posted online as a result of a data scraping that Facebook was aware of since 2019.[7] In total those eight instances over a three-year period resulted in the potential exposure of the personal information of well over 1.5 billion users.

The combination of Facebook's bad data security practices, refusals to act on its own policies, and overall cavalier handling of user data resulted in

1. Facebook has since reorganized into Meta. Press Release, Meta, Introducing Meta: A Social Technology Company (Oct. 28, 2021), https://about.fb.com/news/2021/10/facebook-company-is-now-meta/ [https://perma.cc/29XD-36QL].

2. Michael X. Helligenstein, *Facebook Data Breaches: Full Timeline Through 2022*, FIREWALL TIMES (Jan. 18, 2022), https://firewalltimes.com/facebook-data-breach-timeline/; [https://perma.cc/N5YW-XFQ5].

3. *Id.*

4. *Id.*

5. *Facebook Stored Hundreds of Millions of User Passwords in Plaintext for Years*, KREBSONSECURITY (Mar. 21, 2019), https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/ [https://perma.cc/2TD9-DY4Q].

6. Kurt Wagner, *Facebook admits another blunder with user data*, FORTUNE (July 1, 2020), https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/ [https://perma.cc/SQ8M-JGS2] (Facebook claimed to have fixed this issue in 2018).

7. Emma Bowman, *After Data Breach Exposes 530 Million, Facebook Says it Will Not Notify Users*, NPR (Apr. 9, 2021), https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users [https://perma.cc/K3NC-9BF5].

a $5 billion fine from the Federal Trade Commission (FTC) in 2019.[8] This fine, the largest ever issued by the agency, was still less than one month of revenue for the tech giant.[9] Despite both the fine, and any bad press, Facebook continues to grow, reaching over three billion users in 2023.[10]

As for the affected users, whose data Facebook both relies on and mishandles, their primary relief has come via federal class actions. The most recent of which, relating to the aforementioned FTC fine, resulted in an over 700-million-dollar settlement with affected users.[11] *In re Facebook Internet Tracking Litigation* has been a decade-long saga that threatened to go all the way to the Supreme Court just over the issue of whether or not the suit can proceed.[12] Such lengths and complications are becoming the norm in data breach class actions as courts and advocates alike express concern over their long-term utility compared to agency actions or multi-state challenges.[13]

This skepticism has led to the Supreme Court adopting stringent *actual harm* requirements to show standing in class action suits. As articulated in *TransUnion*, class members now must establish that the harm alleged has a "close relationship" with traditionally recognized harms.[14] This presents a heightened barrier for data breach class actions where judges are reluctant to recognize the harms associated with exposed data such as an increased vulnerability to fraud and anxiety.[15]

Recent commentary has focused on the agency problems inherent to class actions. The low individual stakes for class members result in poor oversight of the actors. This poor oversight enables "sweetheart settlements," wherein class counsel enters defendant favored settlement agreements in exchange for hefty attorney's fees.[16] This is especially problematic because most class actions settle before reaching trial, making class actions less

8. Lesley Fair, *FTC's $5 billion Facebook settlement: Record-breaking and history making*, FTC (July 24, 2019), https://www.ftc.gov/business-guidance/blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-and-history-making [https://perma.cc/DBD5-MWGE].

9. Fair, *supra* note 8; Facebook Reports Second Quarter 2019 Results, META INV.RELS. (July 24, 2019), https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Second-Quarter-2019-Results/default.aspx [https://perma.cc/A377-V839].

10. Dixon, *Number of monthly active Facebook users worldwide as of 3rd quarter 2022*, STATISTA (Oct. 27, 2022), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [https://perma.cc/9WDF-UAH9].

11. In re Facebook Internet Tracking Litig., No. 5:12-md-02314-EJD, 2022 U.S. Dist. LEXIS 205651 (N.D. Cal. Nov. 10, 2022).

12. Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021).

13. *See generally* Elysa M. Dishman, *Class Action Squared: Multistate Actions and Agency Dilemmas*, 96 NOTRE DAME L. REV. 291 (arguing that multistate actions produce better outcomes for class members).

14. TransUnion LLC v. Ramirez, 594 U.S. 413, 417 (2021) ("To have Article III standing to sue in federal court, plaintiffs must demonstrate . . . whether the harm asserted has a 'close relationship' to a harm traditionally recognized as providing the basis for a lawsuit in American courts . . .") (internal citation omitted).

15. *See infra*, Part III.A.

16. John C. Coffee Jr., *Rethinking the Class Action: A Policy Primer on Reform*, 62 IND. L.J. 625, 633 (1987) ("At its simplest, the classic form of opportunism in class actions is the 'sweetheart' settlement, namely one in which plaintiff's attorney trades a high fee award for a low recovery.") (internal citation omitted).

reminiscent of traditional litigation and more akin to negotiations between the class's counsel and defendant's counsel.[17]

To combat these agency issues, judges serve a unique fiduciary role in the class action context, representing the interests of unnamed class members whose rights are bargained away.[18] Presiding judges bear the responsibility of ensuring that class counsel adequately represent the interests of unnamed class members in settlement negotiations.[19] This extends to more than just ensuring that settlement negotiations are at "arms-length," thus absent explicit collusion.[20] Judges must critically examine what, if any, value unnamed class members are receiving as a part of a settlement. This is especially true in the data breach context, where the aforementioned agency problems are amplified, due to the large nebulous nature of the classes, the general undervaluing of data exposure as harm and the overvaluing of non-monetary relief such as *cy pres*, injunctive relief, and credit monitoring.

Data breaches are naturally ideal candidates for class action suits.[21] Generally, data breaches cause small monetary harm to incredibly large groups of individuals.[22] The aggregation of similarly affected individuals is necessary for data breach suits because the low potential for damages makes bringing individual suits impracticable. Data breach class actions also serve an important role in consumer protection, not merely compensating consumers, but also incentivizing corporations to better protect data they otherwise would not see value in protecting.[23] As courts erect increasingly high barriers to data breach class actions, those few that survive take on an elevated level of importance and require a higher judicial standard if they are to continue to serve their purpose.

If federal class actions are to remain an effective means of relief for victims of data breaches, judges must take greater advantage of their role as fiduciaries and examine settlement agreements more skeptically. To that end, judges should adopt a more modern understanding of data breach harms, and

---

17. Bryan G. Garth, *Studying Civil Litigation Through the Class Action*, 62 IND. L.J. 497, 501-04 (1987) (noting that most class actions settle prior to trial, resulting in certification being the focal point of the litigation); Coffee, *supra* note 16, at 627 (suggesting that class actions should be evaluated through the lens of collective bargaining negotiations).

18. *See In re* Dry Max Pampers Litig., 724 F.3d 713, 715 (6th Cir. 2013) ("[C]lass-action settlements affect not only the interests of the parties and counsel who negotiate them, but also the interests of unnamed class members who by definition are not present during the negotiations. And thus there is always the danger that the parties and Counsel will bargain away the interests of unnamed class members in order to maximize their own."); *In re* Baby Prods. Antitrust Litig., 708 F.3d 163, 175 (3d Cir. 2013) (Courts must "make sure that class Counsel are behaving as honest fiduciaries for the class as a whole.) (internal quotation omitted).

19. *In re Baby Products Antitrust Litig.*, 708 F.3d at 175.

20. *See id.* at 1175 (evidence of arms-length negotiations not enough to prove adequacy of representation); Alexandra Lahav, *Fundamental Principles for Class Action Governance*, 37 IND. L. REV. 65, 125 (2003) (arms-length requirement a "poor solution" to concerns over non-adversarial negotiations).

21. *See supra* Part II.A.

22. *See supra* Part II.A.

23. *See Brian T. Fitzpatrick, Do Class Actions Deter Wrongdoing?*, in THE CLASS ACTION EFFECT 183 (Catherine Piche, ed., Editions Yvon Blais, Montreal, 2018).

consequently lower barriers to standing. When examining relief, judges should prioritize long-term change over short-term settlements, and should be particularly skeptical of when a settlement occurs, how the fee awards align interest, and the form of notice from the settlement. Additionally, judges should critically examine non-monetary relief to determine whether unnamed class members are likely to receive appropriate compensation from the settlement.

While there is a healthy debate on whether a model outside of federal class actions should exist to compensate consumer victims of data breaches, this Note does not take a side in the matter. Instead, this Note aims to outline an avenue to improve the efficacy of federal data breach class actions; even if there are alternatives for plaintiff classes, that should not preclude improving the existing system. To that end, this Note begins with a discussion of data breaches, focusing on their key characteristics and the harm associated with exposed PII. The Note then examines class actions, including their requirements and challenges, while paying particular attention to the dual purposes of class actions as compensation and deterrence devices. Following that, the Note then outlines five key potential areas of improvement in data breach class actions: lowering the standing requirement to properly reflect the harms of exposed data, taking a long-term approach when evaluating class members' interests, adopting incentive aligning fee structures, prioritizing the use of e-notice; and more critically examining non-monetary forms of relief.

II. BACKGROUND

A. Characteristics of Data Breaches

A data breach is any unauthorized exposure of sensitive information.[24] Sensitive information encompasses a wide range of data, from what is traditionally viewed as confidential information such as patents and state secrets, to identifying information such as names and addresses.[25] The word *any* in this context, truly means *any*, a data breach is no less a data breach if the information stolen is names and addresses than if it is a state secret.

Data breaches may not require proof that the exposed data was used or even actually stolen.[26] Practically speaking, not all breaches require a hack. Instead, an oversight such as an unsecured login, or unencrypted data set may leave data exposed for an extended period of time, granting access to anyone. In these instances, it may be impossible to show if any data was illegitimately accessed. The data, however, may still be considered exposed and a breach may still be considered to have occurred. This means that a data breach may not require there to be proof of a hacker. Simply leaving sensitive information

24. *What is a Data Breach*, CISCO, (Jan. 20, 2023, 9:55 AM) https://www.cisco.com/c/en/us/products/security/what-is-data-breach.html [https://perma.cc/P794-9367].

25. *Cyber Incidents*, DEP'T. HOMELAND SEC., https://www.dhs.gov/cyber-incidents [https://perma.cc/J5LJ-V2AK] (last visited Jan. 20, 2023, 10:01 AM).

26. *What is a Data Breach, supra* note 24 ("Information that might be stolen or *unintentionally* exposed to unauthorized *viewers*.") (emphasis added).

exposed (as Facebook did in 2019 when they stored passwords in plaintext) constitutes a data breach.[27] Data breaches, consequently, reflect a very traditional understanding of privacy, someone simply seeing your private information is a violation of one's ability to decide the extent to which one's private life is exposed.[28]

In the class action context, data breaches most often refer to exposures of Personally Identifiable Information (PII). PII includes names, addresses, associations, location information, health information and financial information about an individual or group of individuals.[29] The collection and use of PII to create targeted advertisements is the crux of modern Internet transactions and represents the principal monetization model for free services such as Facebook and Twitter.[30] The actual value of PII depends both on the type of data collected and who is using the data. Estimate valuations of all the data Facebook collects on an individual average at around $200 per user.[31] Estimate valuations of user data to criminals largely depend on the volume and type of the information exposed. A single login may be worth as little as a dollar, but a medical file can be valued at up to $1,000.[32]

It is easiest to understand why this large umbrella of data is grouped together when viewed through the lens of a criminal. Every piece of PII, be it the name of someone's dog to someone's fingerprint, enhances a criminal's ability to commit fraud. Take a phishing attack for example. Phishing attacks are a type of social engineering attack that involves the sending of fraudulent communications from a source that appears reputable, tricking the target into acting on behalf of the criminal. For instance, an email claiming to be from your company's HR department requiring you to input your login information to verify or dispute Internet activity allegedly in violation of company policy. This email, which would record your login information and send it to a third party, appears more legitimate if it references a website you actually visit, or a friend you frequently message. Similarly, the classic "prince in need," scam in which a scammer pretends to be a foreign prince who needs a cash advance

---

27. *Facebook Stored Hundreds of Millions of User Passwords in Plaintext for Years*, *supra* note 5.

28. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890) (arguing privacy invasions involve the interference with a persona ability to decide the extent to which personal information is revealed).

29. *Department of Homeland Security Handbook for Safeguarding Sensitive PII*, DEP.'T HOMELAND SEC. (Dec. 4, 2017) https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf [https://perma.cc/W8LY-Y8J6].

30. Kris Gunnars, *How Does Facebook Really Make Money? 7 Main Ways*, STOCK ANALYSIS (Jan. 21, 2023, 10:30 AM) https://stockanalysis.com/article/how-facebook-makes-money/ [perma: https://perma.cc/QQ2Z-3XCA].

31. Robert J. Shaprio, *What Your Data is Really Worth to Facebook*, WASHINGTONIAN MONTHLY (July 12, 2019) https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/ [https://perma.cc/K6RH-JSG4] (calculating the value to Facebook of the data it collects per user is $202).

32. Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/ [https://perma.cc/KU4D-ZVTL].

but will repay you ten-fold can be made more believable if the person needing money is not some far off prince but a distant family member. Viewed through the lens of a criminal, the value of PII is not the immediate harm of possession or access, but the subsequent harms of potentially fraudulent use.

B. The Dual Purposes of Class Actions

Fundamentally, class actions serve to aggregate many individual damages claims into a single lawsuit. This aggregation accomplishes two things: it provides a tool for justice for those who otherwise would be unable to sue, and it keeps businesses in check by discouraging widespread minor abuses over fear of costly suits.[33]

These distinct functions of class actions are inseparable. In the long run, better corporate behavior saves consumers money, and protects them from injustices.[34] In comparison to the actual payouts consumers receive, corporate deterrence may be the more important benefit.[35] This logic underpins the non-monetary relief plaintiffs often receive in class actions, including both injunctive relief and *cy pres* relief, defined as the forfeiture of payouts to class members in favor of payouts to charities or other interest groups.[36] However, because injunctive relief and other non-monetary relief cannot compensate consumers for existing harms, non-monetary relief should not be considered a substitute that can entirely replace direct compensation.[37]

C. Exacerbated Agency Problems Present in Data Breach Class Actions

Like all class actions, data breach class actions incur significant conflicts of interest between clients and attorneys. Similar to other principal-agent relationships, class actions face agency costs, including: (1) the cost of monitoring the agents, (2) the agents' bidding costs, and (3) residual costs of opportunistic behavior.[38] Coined by Professor John C. Coffee Jr., these agency costs have existed since the inception of class actions and most

33. *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF THE LAW 803 (9th ed. 2014) ("[W]hat is most important from an economic standpoint is that the violator be confronted with the costs of his violation--this preserves the deterrent effect of litigation--not that he pay them to his victims.").

34. *See* Russel M. Gold, *Compensation's Role in Deterrence*, 91 NOTRE DAME L. REV. 1997, 2003 (2016) (arguing that deterrence and compensation are intertwined objectives because large cash payouts serve as a form of deterrence not only as fines but by inflicting reputational harm).

35. *See* James D. Cox, *The Social Meaning of Shareholder Suits*, 65 BROOK. L. REV. 3, 39-43 (1999) (arguing that deterrence is a more important goal than compensation).

36. *See* Myriam Giles, *Class Dismissed: Contemporary Judicial Hostility to Small-Claims Consumer Class Actions*, 59 DEPAUL L. REV. 305, 322 (2010) (noting the view of some courts that *cy pres* "distributions confer little or no benefit to class members, but rather serve the broader public interests of . . . deterrence").

37. *See* Frank v. Gaos, 139 S. Ct. 1041, 1047 (2019) ("[*C*]*y pres* payments are not a form of relief to the absent class members and should not be treated as such[.]") (Thomas, J., dissenting).

38. Coffee, *supra* note 16, at 629-30.

traditionally surface in what are called sweetheart settlements, in which class counsel exchange high fees for a lower overall settlement.[39] While sweetheart settlements are possible in any civil litigation, class actions feature exacerbated agency problems. First, class actions tend to have higher information costs because the critical decisions, such as when and for how much to settle, have low visibility. Second, the low overall financial recovery for individual plaintiffs provides little incentive to justify the costs of monitoring settlement negotiations.[40] Third, no public market exists to align the attorney's interest with that of their clients. Consequently, class actions function opposite to normal market activity in which a principal hires their agent.[41] Instead, in class actions, the agent often looks for their principals.[42] Class action attorneys hunt for suitable plaintiffs to bring a profitable suit.[43] As a result, the theoretically aggrieved party, the plaintiff, is likely not as interested in the case as their attorney.[44]

High agency costs have led to two problems: first an overfilling of class actions in the hope to barrel forward settlement agreements as a form of undue influence and the inadequate representation of even well-warranted class actions. Those are distinct problems for the broader system, but for class members they result in the same issue: rights being bargained away in exchange for returns that do not suit their interests.

For courts, these are distinct problems with competing solutions: reducing the number of class actions in order to improve their average quality or alternatively, improving outcomes for class members. On the one hand, having stricter requirements for class certification reduces the number of potential blackmail suits. Conversely, increased fighting over certification drains resources from class representatives increasing defendants' leverage in settlements.[45] In response, courts and the Advisory Committee on Civil Rules of the Judicial Conference of the United States have prioritized curtailing the number of class actions. Consider the 2003 amendments to Federal Rule of Civil Procedure 23, which defines the procedures for federal class actions. These amendments were designed to make certifying classes under Rule 23(b)(3) more arduous by adding an interlocutory appeal provision to the

---

39. *Id.* at 633 ("At its simplest, the classic form of opportunism in class actions is the "sweetheart settlement," namely one in which plaintiff's attorney trades a high fee award for a low recovery.").

40. *Id.* at 630.

41. *Id.* at 629.

42. *Id.*

43. *Id.*

44. John C. Coffee Jr., *The Regulation of Entrepreneurial Litigation: Balancing Fairness and Efficiency in the Large Class Action*, 54 U. CHI. L. REV. 877 882-893 (1987) (characterizing class Counsel as entrepreneurial lawyers, noting the lack of perceived stakes for class members); Alon Klement, *Who Should Guard the Guardians? A New Approach for Monitoring Class Action Lawyers*, 21. REV. LITIG. 25, 27-28 (2002) ("[N]amed representative plaintiffs have proven to be merely figureheads[.]").

45. *See* Bruce Hay, David Rosenberg, "*Sweetheart" and "Blackmail" Settlements in Class Actions: Reality and Remedy*, 75 NOTRE DAME L. REV. 1377, 1390-91 (2000) (arguing that one way to combat sweetheart settlements is to increase standards for certification by minimizing future injury claims).

class certification process.[46] Courts have viewed them even more broadly, seeing the 2003 as a general decree that certification should be increased, and federal courts have imposed more rigorous certification standards as a result.[47]

Expansions of Rule 23(e) have included some efforts to improve the behavior of class counsel. The 2018 amendments to Rule 23(e) now condition the approval of settlements upon demonstrations that the settlement occurred at "arms-length," and that the proposed settlement is "the effectiveness of any proposed method of distributing relief to the class."[48] These rules, however, are entirely based on a judge's discretion, and commentators have criticized these provisions for being too dependent on information presented by attorneys, who may not provide all the information needed to assess the settlement.[49]

Similarly, Rule 23(a)(4) conditions certification on a demonstration that "the representative parties will fairly and adequately protect interests of the class."[50] Like Rule 23(e) this requirement has been criticized as being largely performative.[51] Prior to the lawsuit progressing, there is little way of knowing whether the representative parties will represent the interests of the class. In practice, the only feasible screening question is whether the lawyers are qualified, which in a reversal of the Rule's purpose, means that serial class action lawyers are more likely to be viewed as a party that will represent the interests of the class.[52]

In the data breach context, all of the above issues are compounded. Courts' increasing wariness of data breach harms increases the relative leverage of defendants. Moreover, the lack of oversight and high information costs are greater in the data breach context because absent class members may not understand the actual value of the data taken. This is especially true for plaintiffs who have yet to experience financial harm from a data breach, and thus are not yet invested in proper compensation. Consequently, protecting absent class members becomes an even more judge-centric task.

---

46. FED. R. CIV. P. 23 advisory committee's comments on the 1998 and 2003 amendments

47. John C. Coffee Jr., & Stefan Paulovic, *Class Certification: Developments over the Last Five Years 2002-2007*, 8 CLASS ACTION LITIG. REP. S-787, S-787 (Oct. 26, 2007); *see also* John C. Coffee Jr., *Accountability and Competition in Securities Class Actions: Why "Exit" Works Better than "Voice*," 30 CARDOZO L. REV. 407, 431 (2008) ("Class action certification standards have been significantly tightened across the spectrum of federal court litigation over recent years, and, surprisingly, the most dramatic changes have been in the area of securities class actions.").

48. FED. R. CIV. P. 23(e)(2)(B); FED R. CIV. P. 23(e)(1)(C)(ii).

49. *See generally* Brian Wolfman, *Judges! Stop Deferring to Class-Action Lawyers*, 2 U. MICH. J.L. REFORM 80 (2013) (arguing that judges simply take class counsel at their word when they should not).

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

51. *See* Wolfman, *supra* note 49, at 87.

52. *See generally id.*

III. ANALYSIS

A. Current Stringent Standing Requirements Fail to Reflect the Harms of Data Breaches, and Exacerbate Existing Agency Issues

Class actions must be brought in federal court, which imposes a standing requirement on the plaintiff(s).[53] The standing requirement derives from Article III of the Constitution.[54] In order to bring a case into federal court, a plaintiff bears the burden of satisfying three elements of constitutional standing. First, the plaintiff must have suffered an "injury in fact," a violation of a legally protected interest. The injury alleged must be "actual or imminent, not "conjectural" or "hypothetical."[55] Second, the plaintiff's claim must arise from an injury that is "fairly traceable to the challenged conduct of the defendant."[56] The harm that occurred must be traceable to the defendant's conduct. Third, a favorable court ruling must be able to redress the plaintiff's injury.[57]

As discussed above, the nature of data breaches means that the injury alleged often boils down to an increased risk of harm or fraud.[58] As a result, even in instances of patent wrongdoing on the part of the defendants, many data breach suits fail to even get in the door for lack of standing.[59] This is because courts have been reluctant to acknowledge an increased risk of fraud as a sufficiently imminent injury.[60] In the past two decades, hundreds of cases have been brought alleging improper care of plaintiffs' data resulting in exposure.[61] Most cases, however, have turned not on the handling of the data but on whether or not the exposed data resulted in harm sufficient to grant standing.[62] No matter how deficient defendants' data protection might have been, most cases do not proceed unless plaintiffs show not only that the data was exposed, but that the exposed data was used by the time the suit was brought.

In *Reilly*, plaintiffs alleged that Ceridian had failed to secure its clients' personal data and presented evidence the company not only knew the data was unsecured, but knew that hackers had accessed it.[63] Despite this evidence the court dismissed the case, holding that the plaintiff's allegations of

53. U.S. CONST. art. III.
54. *Id.*
55. Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016).
56. *Id.*
57. *Id.* (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).
58. *Supra* Part II.A.
59. *Supra* Part II.A.
60. *See* Daniele J. Solove, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 739 (2018).
61. *See* Sasha Romanosky et. al., *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 93 (2014).
62. Solove, *supra* note 60, at 739 ("The majority of cases, however, have not turned on whether defendants were at fault. Instead, the cases have been bogged down with the issue of harm.").
63. Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011).

increased harm were mere conjecture that had not yet come true, and thus did not meet the standing requirements.[64] This mindset is pervasive—an increased risk of harm, no matter how apparent, is not enough to grant standing in a majority of lower courts.[65]

This reluctance to acknowledge an increased risk of fraud as an injury in fact has only increased in the wake of the Supreme Court's holding in *Clapper v. Amnesty International*.[66] In *Clapper*, attorneys, journalists, and human-rights activists challenged the constitutionality of a provision of the Foreign Intelligence Surveillance Act, extending the government's authority to conduct surveillance over suspected terrorists.[67] The plaintiffs alleged that they had taken burdensome precautions, including only meeting with clients face to face, out of fear that the government was surveilling their calls.[68] The Supreme Court, however, struck down the case down on the grounds that the plaintiffs had not alleged an "injury in fact," since they had no proof they were being surveilled, and thus brought the harm of traveling those distances upon themselves.[69] The *Clapper* court did note, in a footnote, that the injury in fact may be satisfied if there was a "substantial risk harm would occur."[70]

Where standing has been granted in the wake of *Clapper*, it has been granted on a hybrid theory: if some plaintiffs can show actual harm, then all plaintiffs affected by the breach can demonstrate a "substantial risk harm would occur" to satisfy standing. In *Remijas v. Neiman Marcus Group*, the Seventh Circuit found the risk of harm "immediate and very real" because the data "was in the hands of hackers who used malware to breach the defendant's systems" and "fraudulent charges had shown up on some of its customers."[71] The Ninth Circuit held similarly in *Krottner v. Starbucks Corporation*, conferring standing because there was a subsequent attempt to open a bank account following the data breach.[72]

This hybrid approach faces new challenges in the wake of *TransUnion LLC v. Ramirez*.[73] In *TransUnion*, plaintiffs sued the credit reporting agency TransUnion for violations of the Fair Credit Reporting Act. Due to an oversight in TransUnion's systems, individuals who shared a name with people on the terrorist watch list were incorrectly being flagged as on the

64. *Id.* at 43.

65. *See e.g.*, Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 854 (S.D. Tex. 2015) (holding that the increased risk of future identity theft stemming from data breach not to be a sufficient injury); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 365-66 (M.D. Pa. 2015) (holding that increasing risk of identity theft does not suffice as injury, even though hackers had breached payroll company's computer and accessed personal information).

66. *See generally* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013). (holding that journalissts and activists did not have standing to challenge the Foreign Intelligence Surveillance Act because they had not experienced an injury in fact).

67. *Id.* at 401.

68. Brief for Petitioners at 10, 35, *Clapper*, 568 U.S. 398 (No. 11-1025).

69. *Clapper*, 568 U.S. at 422.

70. *Id.* at 414-15 n.5.

71. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693-94 (7th Cir. 2015) (acknowledging that plaintiffs were "careful" to point out instances of fraud already occurring).

72. Krottner v. Starbucks Corp., 628 F.3d 1139, 1142-43 (9th Cir. 2010).

73. *TransUnion LLC*, 141 S. Ct. 2190.

watch list.[74] A class of over 8,000 individuals whom TransUnion warned were affected, and who were not given notice of their rights pursuant to the Fair Credit Reporting Act sued.[75] The court held that of the over 8,000 class members who had misleading credit reports, only the 1,853 who could show that they suffered reputational harm as a result had standing to sue.[76] The crux of the majority's holding dealt with a "close relationship" standard in which plaintiffs now have to show that the harm alleged is closely related to a traditionally recognized harm, another barrier to data breach class actions.[77] Equally concerning is the Court's division of the class to only those who had already suffered the harm because it calls into question whether the hybrid theory still holds.

Like *Clapper* before, a narrow reading of *TransUnion* should not close the door on an increased risk of future harm granting standing. In *TransUnion* the increased risk of harm was not actually at issue, those plaintiffs who did not already suffer reputational harm were unlikely to do so since TransUnion had fixed the error.[78] This separates the harm in *TransUnion* from that of a data breach, since once data is exposed and taken it cannot be reversed. Even fraud protection does not catch everything, so hackers having data always increases the risk of harm. Still, the potential for a blanket reading of *TransUnion* is dangerous and could present yet another barrier to data breach class actions.

TransUnion poses a more speculative harm to data breach class actions. While an increased risk of fraud is the primary form of harm from a data breach, there is a second form of harm: increased anxiety as a result of a privacy violation.[79] As the definition of a data breach itself acknowledges, simply having personal information exposed is a privacy violation.[80] This is most obvious when the information is sensitive. Having personal medical information potentially exposed for instance, creates anxiety. Any data breach can and often does result in anxiety as people are justifiably afraid of leaks of data or fraudulent transactions.[81] While many people have identity theft and fraud protection, no system is perfect and consumers who know their data has been breached have to pay greater attention to every transaction on their accounts. The data breach is the direct cause of this anxiety.

The law has grown to recognize anxiety, and other so-called "ethereal" harms in other areas. Warren and Brandeis, progenitors of the modern privacy torts catalogued this change. Assault, for instance, signifies

---

74. *Id*. at 2191.
75. *Id*.
76. *Id.* at 2214.
77. *See id.* at 2204.
78. *See id.*
79. Solove, *supra* note 60, at 739 ("The majority of cases, however, have not turned on whether defendants were at fault. Instead, the cases have been bogged down with the issue of harm.").
80. *What is a Data Breach*, CISCO, (Jan. 20, 2023, 9:55 AM) https://www.cisco.com/c/en/us/products/security/what-is-data-breach.html [https://perma.cc/P794-9367].
81. Solove, *supra* note 60, at 739; *see also Krottner*, 628 F.3d at 1142-43 (acknowledging that plaintiffs do justifiably feel an increased anxiety from the potential of a breach).

the recognition of a harm caused by the anxiety produced by fear. Modern law also recognizes infliction of emotional distress as a harm, and breaches of confidentiality as a harm. In case after case involving violations of privacy, courts cite fear of humiliation or embarrassment and the increased anxiety that comes with it as the basis for damages.

Unfortunately, courts have yet to apply privacy torts to the data breach context.[82] As leading information privacy law expert Daniel Solove puts it, "the inconsistency between these different contexts is quite stark."[83] Even still, this can and should provide a secondary ground upon which standing can be granted. In cases in which particularly sensitive data was definitively exposed, standing should be granted. Thought of another way, recognizing the potential humiliation and anxiety associated with exposed data is crucial to the deterrence function of class actions. Corporations should be more incentivized to protect more sensitive data. While this is reflected in the potential damages associated with more sensitive data, having this also be reflected in the ability for suits involving sensitive data to be granted standing reinforces this purpose.

B. Judges as Fiduciaries Should Prioritize Plaintiff Favored Settlements Over Immediate Payouts.

Despite its flaws, Rule 23(e) grants judges broad discretion to determine whether to approve a settlement. In essence, Rule 23(e) empowers judges to act as fiduciaries. Judges take a more active role in class action litigation than they do in individual litigation. For example, judges must decide whether the case will proceed as a class action on behalf of absent parties. In making this decision, judges must also decide who represents the class, whether and on what terms class members will settle, and how much the class will pay its counsel. Determining damages and settlements is particularly important in the judge's fiduciary role. As explained by the Sixth Circuit,

> [c]lass-action settlements are different from other settlements. The parties to an ordinary settlement bargain away only their own rights—which is why ordinary settlements do not require court approval. In contrast, class-action settlements affect not only the interests of the parties and counsel who negotiate them, but also the interests of unnamed class members who by definition are not present during the negotiations. And thus, there is always the danger that the parties and counsel will bargain away the interests of unnamed class members in order to maximize their own.[84]

82. Solove, *supra* note 60, at 771.
83. *Id.*
84. *In re Dry Max Pampers Litig.*, 724 F.3d at 715.

Accordingly, courts fill a fiduciary function on behalf of absent class members to ensure that class counsel are "behaving as honest fiduciaries for the class as a whole."[85] Rule 23(e) provides a basic framework for the way judges should treat this duty. First, Rule 23(e) makes clear that the judge's role involves more than ensuring negotiations are conducted at arms-length; the proposed settlement must additionally "fairly and adequately protect interests of the class."[86] As stated by the American Law Institute (ALI), "in reviewing a proposed settlement, a court should not apply any presumption that the settlement is fair and reasonable."[87] This means judges should not, as critics point out they do, simply take attorneys at their word.[88]

The Restatement (Third) of the Law of Agency states that agents should do what their principals would "reasonably" want them to do absent explicate instruction otherwise.[89] This means judges must act as rational class members who intend to maximize their recovery from the suit.[90] Considering the two goals of class actions, maximizing recovery means more than maximizing immediate payouts; instead reasonable fiduciaries must also ensure that the settlement still serves as adequate deterrence against future bad behavior. This suggests that the rational class member would not prioritize a quick payout over a plaintiff favored settlement. Judges as fiduciaries, then, must heavily guard against premature settlements.[91]

C. In Order to Mitigate Agency Problems, Judges Should Prioritize Fee Awards Which Align the Incentives of Class Counsel and Class.

In pursuit of these macro-level objectives, there are several key micro-level considerations judges must make, perhaps the most important being what fee awards class counsel should be entitled to. There are two primary methods to calculate fees. The first of which is the lodestar method, which aims to directly reward time investment.[92] Under this fee calculation method, courts award attorney's fees by multiplying the number of hours class counsel expended on the litigation by a reasonable hourly rate for the region and

85. *In re Baby Prods. Antitrust Litig.*, 708 F.3d at 175.

86. FED R. CIV. P. 23(e)(1)(C)(ii).

87. Am. Law Institute, Principles of the Law of Aggregate Litig. § 3.05(c) (2010).

88. *See generally* Wolfman, *supra* note 49 (arguing that judges simply take class counsel at their word when they should not).

89. RESTATEMENT (THIRD) OF THE L. OF AGENCY § 8.01; RESTATEMENT (THIRD) OF L. OF AGENCY § 2.02 cmt. B ("The agent's fiduciary duty to the principal obliges the agent to interpret the principal's manifestations so as to infer, in a reasonable manner, what the principal desires to be done in light of facts of which the agent has notice at the time of acting.").

90. *See generally* Brian T. Fitzpatrick, *A Fiduciary Judge's Guide to Awarding Fees in Class Actions*, 89 FORDHAM L. REV. 1151 (2021).

91. *See id.* at 1153 (finding that at least sophisticated clients largely prefer to monitor against premature settlements rather prioritize expediency).

92. *See in re* Bluetooth Headset Prod. Liab. Litig., 654 F.3d 935, 942-43 (9th Cir. 2011) (defining lodestar method and reversing trial court's award of a fee using lodestar method where the trial court made no calculation of the lodestar amount).

experience of the lawyer.[93] Judges in this method have discretion to award a multiplier based on the circumstances.[94] The second method is the percentage method whereby courts select a percentage of the ascertainable common fund or the common benefit to award as a fee.[95]

Regardless of fee method, there are statutory restraints on the maximum compensation. Many jurisdictions have created a cap on fee awards at only twenty-five percent of any recovery, with some reducing that percentage if the recovery is more than $100 million.[96] While this is a trend, a study of eighty data breach settlements from 2010 to 2020 found that the average proportion of attorney's fees to the total settlement fund was 35.06%.[97] Relative to class actions as a whole this number is high, as a 2004 study found that the mean attorney's fees in class actions generally was only 21.9%.[98]

Because judges have discretion to approve attorneys' fees, they have discretion to examine how well the attorney's fees align the interests of plaintiffs with their counsels. Rule 23(e) was amended in 2018 to explicitly require consideration of "the effectiveness of any proposed method of distributing relief to the class" and assurance the class's recovery is commensurate with "the terms of any proposed award of attorney's fees."[99] Applying economic models to the question of what judges should do in class action, Professor Brian T. Fitzpatrick proposes either a payment model based a) on a fixed or escalating percentage of the recovery, or (b) a percentage of the recovery plus a contingent lodestar.[100] Both recovery methods help guard against premature settlement.[101] Though not discussed by Fitzpatrick, a second benefit of such recovery methods is that they could potentially discourage ineffective forms of non-monetary recovery such as injunctive or *cy pres* by helping prioritize purely monetary recovery. Moreover, the contingent lodestar method would enable judges to tie awards to areas such as payout rate, forcing class counsel to demand better notice when they otherwise would not be incentivized to do so.[102]

None of the above is to say that these methods are the only acceptable forms of fee awards. Instead, Fitzpatrick's proposals present a model for examining attorneys through the lens of interest alignment. Making these calculations is risky for judges as fiduciaries who both want to maximize class members' value and ensure that class counsel is properly compensated for their work, incentivizing future class action suits. The lengthy and costly

93. Morris A. Ratner, *Class Counsel as Litigation Funders*, 28 GEO. J. LEGAL ETHICS 272, 280 (2015).

94. *Id.*

95. *Id.*

96. *See* Torrisi v. Tucson Elec. Power Co., 8 F.3d 1370, 1376 (9th Cir. 1993) ("In common fund cases such as this, we have established 25% of the common fund as the 'benchmark' award for attorney fees.") (internal citation omitted).

97. Katherine Cienkus, *Privacy Class Action Settlement Trends: Industry Practice or Improper Incentives?*, 40 REV. LITIG. BRIEF 1, 33 (2021).

98. *Id.* at 34

99. FED. R. CIV. P. 23(e).

100. Fitzpatrick, *supra* note 90, at 1163.

101. *Id.* at 1164.

102. *Id*.

proceedings of a class action mean that class counsel often devote large amounts of time and money to pursuing the suit. These are not risk-free undertakings and class counsel is not guaranteed a payout from the suit. The result is that no matter which method, loadstar or percentage, is used, courts often factor in time expended when evaluating reasonability.[103] This opens the door for a system in which class counsels favor time-intensive rather than cost-intensive cases, inadvertently exacerbating the agency problem and leading to premature settlements right before expensive points in a case (e.g. right before having to hire expensive expert witnesses).[104] Like evaluating the settlement as a whole, when evaluating fees, judges must be wary of not just what the settlement was but when the settlement was made.

D. Within Their Fiduciary Capacity, Judges Should Follow Notice Best Practice, Including Expanded Use of e-Notice, and Easy to Understand Language.

Rule 23 requires that any settlement feature the "best notice practicable under the circumstances."[105] The Supreme Court crystallized its notice preferences in *Eisen v. Carlisle and Jacqueline*, requiring that "individual notice… be sent to all class members who can be identified with reasonable effort."[106] In an ideal world, this would mean every single class member receives direct notice of a settlement. In the modern world of large-scale litigation, particularly data breach litigation, where class sizes can be well over 100 million and whose members are often ambiguous, clear direct notice to all class members is unrealistic. Unfortunately, this gap between what is ideal and what is possible has led to inaction by courts, who have largely failed to embrace e-notice, or critically examine the actual language of the notice, two common sense improvements to notice requirements.[107] This is problematic because notice is inseparable from claims, as the Supreme Court explained in *Eisen*, notice is "the touchstone of due process."[108] The 2018 Amendments to Rule 23 somewhat acknowledge these problems, requiring judges to now consider "the effectiveness of any proposed method of disturbing relief to the class."[109]

The Advisory Committee has codified its concern over the language of notices in Rule 23(e)(2)(C)(ii) requiring that "The notice must be clearly and concisely stated in plain, easily understood language."[110] Despite this, courts rarely examine the language of a notice, and notices are often still

103. *Ratner*, *supra* note 93, at 280.
104. *Id.*
105. FED. R. CIV. P. 23(c)(2)(B).
106. Eisen v. Carlisle & Jacquelin, 417 U.S. 156, 156-58 (1974).
107. *See* Robin J. Effron, *The Invisible Circumstances of Notice* 99 N.C. L. REV. 1521, 1534-38 (2021) (arguing that subpar notice examination is a function of courts stubborn preference on letter mail).
108. *Eisen*, 417 U.S. at 173-74 (interpreting the Advisory Committees' notice requirements as serving the requirements of due process).
109. FED. R. CIV. P. 23(e)(2)(C)(ii).
110. *Id.* at 23(c)(2)(B).

indecipherable for the layperson.[111] This is not merely a conceptual problem, data supports the conclusion that simplified notices of settlement improve claims rates. A 2019 FTC study examining claims rates in consumer fraud class actions found that the "claims rate was higher in cases where the notices used visually prominent, 'plain English' language to describe payment availability."[112] Despite this the FTC found that only forty percent of the notices they reviewed contained plain English payment language, and even less of those were concise.[113] This is consistent with the findings of contemporary scholarship which suggests that language examination rarely occurs.[114]

E-notice also represents an avenue of growth for courts. Like plain language, the effect of e-notice is both conceptually and empirically clear. If more *potential* class members receive notice, then consequently more *actual* class members will receive the notice. The best way to see this effect is through class action objectors, who "are almost twice as common in cases involving E-Notice."[115] Objectors serve a key role as guardians of unnamed class members, objecting to settlements on behalf of class members who feel they are not being adequately compensated. The presence of class action objectors is an important factor for courts, as their presence serves as yet another check on potentially self-serving practices by class counsel at the expense of unnamed class members. Their presence also indicates an area where expanded notice may be in the interest of unnamed class members but not in the interest of class counsel. Still, e-notice has been an area of innovation in recent years, largely driven by plaintiffs' attorneys. The use of social media and targeted advertising for notice have both expanded.[116]

In the data breach context, direct notice is rarely possible for most class members, but intermediate improvements to the notice and language of notices can be tremendously impactful. Because overall cyber literacy is low, it is even easier to turn potential claimants away by drowning them in technical language. The lack of use of e-notice like targeted advertising is especially perplexing in the data breach context where users of a breach can be notified when they visit the site.

E. When Evaluating Remedies, Judges Should Strongly Disfavor Injunctive, Cy Pres, and Credit Monitoring as Forms of Relief.

Rule 23(e) empowers judges to examine remedies. That extends to more than just accepting the purported cost of a remedy to defendants, but also the actual remedy generated for class members. Thus, improving settlement outcomes requires an understanding of what remedies to a data

111. Lahav, *supra* note 20, at 84-85 (noting that some many notice agreements are "inaccessible to a reader trained as an attorney").

112. F.T.C., CONSUMER AND CLASS ACTIONS: A RETROSPECTIVE AND ANALYSIS OF SETTLEMENT CAMPAIGNS 1-2 (2019).

113. *Id*. at 35.

114. Lahav, *supra* note 20, at 84-85.

115. Christine P. Bartholomew, *E-Notice*, 68 DUKE L.J. 217, 258 (2018).

116. *See* Effron, *supra* note 107, at 1557-58.

breach are possible and appropriate. Generally, there are five forms of relief in federal data breach class actions: credit monitoring and fraud protection, direct cash payouts, coupons, *cy pres*, and injunctive relief.[117] Each form of relief has its own appeal, and there is no right combination of remedies for every case. For fiduciaries, each form of remedy requires its own analysis and should raise its own set of red flags. Much like choosing your own adventure game, when presented with a certain type of remedy a certain problem should be examined.

1. Credit Monitoring and Fraud Protection

When the harm from a data breach primarily is the increased risk of fraud, identity theft protection and credit monitoring represent an obvious value to consumers. The value of this remedy, however, is contingent on whether the settlement happened at a timely point relative to the breach and whether the consumers in question already had identity theft protection. If for instance, the settlement did not occur until five years after the suit in question, many of the victims may already have been defrauded rendering the protection useless. In many instances, corporations preemptively offer identity theft protection when notified of a breach, and many banks and credit agencies offer identity theft protection as a perk.[118] Even if consumers do not already have identity theft protection through a bank or credit agency, they likely do so through another suit. Currently there are at least eleven suits of class sizes of over one million individuals in which credit monitoring was a

117. *See* Cienkus, *supra* note 97, at 14-24 (conducting analysis on prevalence of the major relief types in privacy class actions).

118. Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113, 125-28 (2011) (commenting on the trend of voluntarily offering credit-monitoring after a breach); *See also*, *RedCard Benefits & Identity Services*, TARGET (Jan. 22, 2023, 10:41 PM) https://www.target.com/c/redcard-benefits-identity-safeguards/-/N-4srzk, [https://perma.cc/36FL-8P53] (Target's RedCard identity protection guide details identity protection services included with the card such as fraudulent purchase alerts.).

part of the settlement and that credit monitoring is still active.[119] This is not including the settlements for *In re Yahoo Inc.* and *In re Capital One Inc. Customer Data Security Breach Litigation*, each of which are on appeal or have final approval pending but would include credit monitoring for 194 million people and ninety-eight million people respectively.[120] Though overlap is unknown at this point there are theoretically 568 million people who have or will have access to credit monitoring through class actions, which is almost double the population of the United States. This calls into question whether credit monitoring has any value. At the very least, judges should look at it skeptically. If class counsel cannot prove that this is a value-add to class members, then it should not be treated as one.

2. Direct Cash Payments

By far the most common form of compensation from data breach suits is direct cash payments.[121] Largely this is the remedy preferred by commentators and judges. Section 3.07(a) of the American Law Institute Principles succinctly states: "If individual class members can be identified through reasonable effort, and the distributions are sufficiently large to make individual distributions economically viable, settlement proceeds should be distributed directly to individual class members."[122] This rule follows from the principle that "[t]he settlement-fund proceeds, generated by the value of

119. *In re* Equifax Inc. Customer Data Sec. Breach Litig., No. 17-md-2800-TWT, 2020 U.S. Dist. LEXIS 7841, at *152 (N.D. Jan. 13, 2020) (194 million affected individuals, two year minimum credit monitoring or reimbursement of credit monitoring); *In re* Experian Data Breach Litig., No. 15-cv-01592 AG, 2019 U.S. Dist. LEXIS 81243, at *19 (C.D. Cal. May 10, 2019) (Fifteen million affected individuals, two years of credit monitoring); *In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 15-md-2633-SI, 2019 U.S. Dist. LEXIS 127093, at *66 (D. Or. July 29, 2019) (10.6 million affected individuals, two years of credit monitoring); Adlouni v. UCLA Health Sys. Auxiliary, No. BC 589243, 2015 WL 13827028, at *19 (Cal. July 25, 2019) (4.5 million affected individuals, two years of credit monitoring); Atkinson v. Minted, Inc., No. 3:20-cv-03869-VC, 2021 WL 6028374 (N.D. Cal. Dec. 17, 2021) (4.1 million affected individuals, two years of credit monitoring); Cochran v. Kroger Co., No. 21-cv-01887-EJD, 2021 WL 6028374, at *14 (N.D. Cal. Mar. 24, 2022) (3.82 million affected individuals, at least three years of credit monitoring); *In re* Med. Informatics Engi'g, Inc., Customer Data Sec. Breach Litig., No. 315-md-2667, Dkt. 192, 3 (N.D. Ind. Jan. 30, 2020) (More than three million estimated affected individuals, two years of credit monitoring); *In re* Banner Health Data Breach Litig., No. 2:16-cv-02696-PHX, 2020 WL 12574227 (D. Ariz. Apr. 21, 2020) (slip copy) (2.9 million affected individuals, two years of credit monitoring); *In re* 21st Century Oncology Customer Data Sec. Breach Litig., 380 F. Supp. 3d 1243, 1245 (M.D. Fla. Mar. 11, 2019) (2.2 million affected individuals, two years of credit monitoring); Fox v. Iowa Health Sys., No. 3:18-cv-00327-JDP, 2021 WL 826741, *11-12 (W.D. Wis. Mar. 4, 2021) (1.4 million affected individuals, one year of credit monitoring, deferable for up to one year).

120. *In re* Yahoo Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2020 U.S. Dist. LEXIS 129939, at *50, *89 (N.D. Cal. July 22, 2020); *In re* Cap. One Inc. Customer Data Sec. Breach Litig., No. 19-md-2915, 2022 U.S. Dist. LEXIS 234943 (E.D. Va. Sept. 13, 2022).

121. *See* Cienkus, *supra* note 97, at 21.

122. *In re* BankAmerica Corp. Sec. Litig., 775 F.3d 1060, 1063 (8th Cir. 2015) (citing ALI Principles §3.07 cmt. (b)) at n. 15).

the class members' claims, belong solely to the class members."[123] The actual amount consumers receive not only depends on the total settlement fund, but whether the compensation model is fixed or varied based on the total number of payments.[124] Most commonly, the total cash each consumer would receive was fixed regardless of the total size of the settlement fund, though in a minority of instances damages were awarded based on the total number of claims, or based on which tier of plaintiff a class member fell into.[125] These latter forms of settlement divide class members into tiers based on the harm suffered, e.g. whether a fraudulent charge actually occurred.[126]

Large settlements present a theoretical but overstated problem for direct cash payment remedies. *Fraley v. Facebook Inc.* presents an example of how this problem is overstated.[127] The parties initially proposed a *cy pres*-only settlement for the class of 100 million individuals alleging that cash distributions "[are] simply not practicable in this case, given the size of the class."[128] This complaint was rebuffed by Judge Seeborg, demanding a new proposal on the grounds that size alone did not prove infeasibility.[129] In the end, the parties settled on a restructured-claims-made settlement which distributed funds directly to the class.[130] Suggestions that direct cash settlements would not work might indicate a deeper problem in the lawsuit, questioning whether a class action was the proper form of suit. Any reluctance on the part of class counsel to enter a settlement with direct cash payouts suggests that either class counsel is not adequately representing the interests of class members or that there is a fundamental problem with the suit.

3. Coupons

Coupon settlements provide compensatory monetary rewards in the form of vouchers for a given company.[131] Functionally, they are the same as direct cash payouts, except that they provide only limited value to claimants. Coupon settlements have largely fallen out of favor after the Class Action Fairness Act of 2005 added the requirement that attorney's fees be based "on the value to class members of the coupons that are *redeemed*."[132] Therefore, even if a coupon settlement with 20,000 members all received a $10 coupon is valued at $200,000, attorneys' fees cannot be calculated until coupons are redeemed. Coupons generally have an incredibly low redemption rate, as unlike in a direct cash payment there is both an acquisition and a use barrier

123. Klier v. Elf Atochem N. Am., Inc., 658 F.3d 468, 474 (5th Cir. 2011) (citing ALI Principles §3.07 cmt. (b)) at n. 15).

124. *See* Cienkus, *supra* note 97, at 14-24.

125. *See id.*

126. *See id.*

127. Fraley v. Facebook, No. C 11-1726 RS, 2012 WL 5835366, *6 (N.D. Cal. Aug. 17, 2012).

128. *Id*. at 1.

129. *Id*. at 2.

130. *Id*.

131. *See* Cienkus, *supra* note 97, at 16-18.

132. 28 U.S.C. § 1712(a) (emphasis added).

to the class member. For example, in *Montferrat v. Container Store, Inc.* only about 1,600 of the 87,000 class members submitted claims for coupons.[133]

4. Cy Pres

Cy pres settlements are those which substitute small payments to consumers for payments to third parties, usually charities that support data privacy causes or to university boards.[134] These settlements have a certain appeal when viewed through the lens of improving the industry. By supporting charities, data privacy causes will theoretically receive more public support. Between 2010 and 2020 there were eighty privacy settlements that substituted compensation for class with *cy pres* relief (usually in conjunction with injunctive relief). A benefit of *cy pres* relief is that the damages a company faces are not contingent on the actual redemption rate of class members.

Cy pres settlements are not without controversy, particularly in instances in which they take the place of monetary reward.[135] Because they do not actually compensate class members many courts now view *cy pres* settlements as an avenue of last resort. Moreover, *cy pres* settlements exacerbate the aforementioned agency problem because the inclusion of a *cy pres* distribution may increase a settlement fund, and thus attorneys' fees, without providing any benefit to the class.[136] *Cy pres* settlements also create a new set of agency problems when the targeted recipients are already recipients of funds from the defendants.[137] *Cy pres* settlements, then, require heightened scrutiny, since they deprive class members of direct compensation while opening numerous avenues for conflicts of interest.

5. Injunctive Relief

Injunctive relief is the most included feature in settlements, usually alongside compensation. The focal points of multiple settlements have included commitments to update privacy policies, and increase security measures to avoid a similar breach. If direct cash payments serve the goal of compensating plaintiffs for harm, injunctive relief serves class action's second goal of cleaning up industries. The problem is that often class actions substitute injunctive relief for compensation. Take *In re Yahoo Mail Litigation* in which the attorney's fees constituted almost all of the settlement,

133. *See* Cienkus, *supra* note 97, at 17-18 (looking at the claims rate of *Monteferrante* to discuss disfavoring of coupons settlements).

134. *See id.* at 19.

135. *See id.* at 21.; *See e.g.*, *In re* BankAmerica Corp. Secs. Litig., 775 F.3d at 1063 (Many courts "have criticized and severely restricted" *cy pres*.).

136. *Frank*, 139 S. Ct. at 1047 (Thomas, J., dissenting) ("[*C*]*y pres* payments are not a form of relief to the absent class members and should not be treated as such[.]").

137. Renewed Objection of Theodore Frank, *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 934 F.3d 316, 320 (3d Cir. 2019) (proposed *cy pres* university boards were recipients of funds already from defendant, members of class Counsel also sat on selected boards).

but required Yahoo to make technical changes to how it analyzed user emails for advertising purposes.[138] While this sounds like a case of a class action fulfilling its goal, it relies on a myriad of faulty assumptions. For one, assuming an injunctive has monetary value to plaintiffs requires one to assume that corporations would not make these changes *absent* the relief. This assumption is particularly weak in the case of large corporations, since a large settlement in and of itself would likely cause them to make the technical changes to prevent future suits. In those instances, by including injunctive relief as a part of the overall value of the settlement, defendants are in essence forcing plaintiffs to pay for something defendants would have likely chosen to do anyway. In some instances, changes to policies simply do not matter. Again, take Facebook, between 2018 and 2022 three of Facebook's major incidents were repeat offenses of things the company claimed to have fixed. Injunctive relief, then, is no relief.

IV. CONCLUSION

Data breaches are ideal class action suits. The aggregation of the many small damages claims resulting from a data breach into a single suit is the only viable form of compensation for consumers, and an important deterrence to bad corporate behavior. Though ideal, data breach class actions have become victims of the growing wave of hostility against federal class actions. Increased standing requirements that fail to reflect the actual harm of data breaches are increasingly preventing data breach class actions from proceeding. Those that do proceed suffer from increased agency problems due to a lack of understanding of data breach harms and remedies which makes it harder to spot bad settlements. Data breach class actions are not a lost cause, Rule 23(e)'s empowering of judges as fiduciaries can mitigate the aforementioned agency problems with only minor changes. For one, judges do not have to be so stringent in standing requirements. Adopting a more modern understanding of data breach harms as not only substantially increasing the risk of future harm, but also as being violations of consumer's privacy which cause mental anguish would let more suits in the door and help increase the relative bargaining power of the class. When evaluating settlements, judges should keep in mind the dual purposes of class actions as compensation and deterrence devices, and thus prioritize plaintiff favored settlements over expedient ones, while being mindful of premature settlements. Judges should also critically examine fee award structures and ask not simply whether the compensation is fair but whether the proposed fee award actually aligns incentives. Judges should also evaluate notice requirements critically to ensure maximum possible notice, data breaches are ideal candidates for the expanded use of e-notice. Finally, judges should be more critical of non-monetary remedies, strongly disfavoring credit monitoring, cy pres and injunctive relief.

138. *In re* Yahoo Mail Litig., No. 13-CV-4980-LHK, 2016 U.S. Dist. LEXIS 115056, *12 (N.D. Cal. Aug. 25, 2016).