ALM | LAW.COM

New York Law Journal

Can I Settle In Federal Court After All? A Data Breach Class Action Case Study

By Judith A. Archer, Sean Topping, Alexis Braun and Audrey Faulks

October 8, 2025

Executive Summary

Data breach-related class actions are a mainstay in U.S. courts and do not appear to be going away any time soon. As with civil litigation generally, most such cases settle rather than proceed to trial.

Data breach class actions settled in federal court, however, can give rise to interesting jurisdictional issues, such as whether a court can order and oversee a settlement where plaintiffs' standing has previously been challenged. Such considerations complicate an already complex legal calculus for both where plaintiffs should file and defendants must defend data breach class actions.

This article examines how procedural hurdles, like standing requirements, are shaping the trajectory of data breach class action settlements in courts across the country.

Data Breach Class Action Litigation: An Overview

In recent years a flurry of putative data breach class actions have been brought against companies that purportedly acquired, stored, and/or used Personally Identifying Information (PII) and other sensitive information impacted in a data breach. In 2024 alone, over 1,488 data breach class actions were filed, a figure that has nearly tripled since 2022. *Class Action Lawsuits in Data Breaches: A 2025 Legal Compliance Guide*, Compliance Hub (Feb. 15, 2025).

Multi-District Litigations (MDLs), like those involving the MOVEit breach, which contained "more than 300 cases against various configurations of Defendants," demonstrates the increasing complexity and scale



Cybersecurity risk #4: Data privacy

of data breach litigation. *In Re: MOVEit Data Sec. Breach Litigat.*, MDL No. 1:23-md-03083, 2024 WL 5092276, at *2 (D. Mass. Dec. 12, 2024).

While data breach class actions may range in complexity, they typically follow a predictable pattern: a data incident occurs (often perpetrated by cybercriminals or "threat actors"); the impacted entity notifies regulators and individuals whose PII may have been exposed; individuals come forward as purported class representatives; plaintiffs' attorneys file class actions asserting claims based on common law claim, *e.g.*, negligence, unjust enrichment, breach of implied contract, and statutory claims. Where multiple class actions are filed, the cases are usually either consolidated or coordinated in an MDL.

The cases then proceed through dispositive motion practice, often involving motions to dismiss for lack of subject matter jurisdiction (*i.e.*, Article III standing) and/or failure to state a claim,

as well as potential motions to compel arbitration where applicable. If any claims survive, briefing and discovery re class certification and/or the merits follow.

Data Breach Class Actions Frequently Settle

Data breach class actions, however, are frequently resolved through settlements, driven by factors such as the complexity of large, dispersed plaintiff classes with relatively limited alleged damages, as well as the substantial litigation costs and risks faced by both plaintiffs' firms and defendants.

Recent, high profile data breach class action settlements include *In Re Alphabet, Inc. Securities Litigation*, No. 18-cv-06245 (N.D. Cal. filed Oct. 11, 2018), which arose from an alleged data breach that exposed Google+ users data and resulted in a $350 million settlement with Alphabet Inc. *see also* Jonathan Stempel, *Google to pay $350 million to settle shareholders' data privacy lawsuit*, Reuters (Feb. 6, 2024).

Such settlements generally include relief on a claims-made basis wherein participating settlement class members receive some form of direct monetary relief, often in addition to credit/fraud monitoring and data security commitments from the impacted entity.

They also must be approved and administered by the court. *See, e.g.*, Fed. Civ. R. P. 23(e) ("The claims, issues, or defenses of a certified class—or a class proposed to be certified for purposes of settlement—may be settled, voluntarily dismissed, or compromised only with the court's approval."); NY CPLR 908 ("A class action shall not be dismissed, discontinued, or compromised without the approval of the court."). While court review may seem perfunctory, it has the potential to impose significant hurdles for preliminary and/or final approval of a class settlement.

The Legacy of 'Frank v. Gaos': Jurisdictional Scrutiny Over Class Action Settlements

One such hurdle is subject matter jurisdiction, which the U.S. Supreme Court and lower courts have held should be evaluated prior to approving a class action settlement. Federal courts may lack subject matter jurisdiction where, for example, plaintiffs fail to demonstrate that they have standing pursuant to Article III of the U.S. Constitution.

The Supreme Court has made clear that courts have a duty "to assure [them]selves of litigants' standing under Article III." *See DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 340 (2006) (quoting *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180 (2000)).

The same obligation applies for approval of class action settlements. *See Frank v. Gaos*, 586 U.S. 485 (2019). In *Frank v. Gaos*, plaintiffs in a putative class action against the operator of a search engine website asserted claims under the Stored Communications Act and state law that the operator violated users' privacy by disclosing their internet search terms to owners of third-party websites. After repeated rounds of dispositive briefing, the Northern District of California preliminarily approved a *cy-pres* only settlement, which the Ninth Circuit Court of Appeals affirmed.

Rather than considering the merits, the Supreme Court vacated the judgment and remanded to determine whether any named plaintiff suffered an injury-in-fact, as required for Article III standing (an analysis neither the district nor appeals court had performed).

Frank v. Gaos presents an issue unique to data breach class action litigation. Article III standing is frequently challenged in data breach cases. *See, e.g.*, *In re Unite Here Data Sec. Incident Litig.*, 740 F. Supp. 3d 364, 375 (S.D.N.Y. 2024) (concluding that union members "have alleged a sufficiently substantial risk of future identity theft and medical fraud to confer standing."); *Cantinieri v. Verisk Analytics, LLC*, No. 2:21-cv-6911, 2024 WL 5202579, at *12 (E.D.N.Y. Dec. 23, 2024) (discussing that disclosure of plaintiff's PII to an unauthorized entity, by itself, did not establish standing).

Yet, following hard-fought settlement negotiations, the parties must then turn to the same court to approve the settlement.

To no one's surprise, parties may be loath to raise subject matter jurisdiction, and may even try to concede the court has jurisdiction to approve the class action settlement. Despite *Gaos'* holding, courts often approve settlements where standing has been previously challenged with little-to-no inquiry into their own jurisdiction. *See, e.g.*, *In re Practice Resources, LLC Data Security Breach Litigation*, No. 6:22-cv-00890 (N.D.N.Y. filed Aug. 25, 2022); *Pan v. Atlas Real Estate Group Llc.*, No. 1:23-cv-910 (D.

Colo. filed Apr. 12, 2023); *Bahnmaier v. Wichita State University*, No. 2:20-cv-2246 (D. Kan. filed May 14, 2020) (all approving settlements despite pending motions to dismiss for lack of Article III standing).

Some courts have begun to rigorously evaluate whether they have subject matter jurisdiction prior to approving data breach class action settlement. One such example from the Southern District of New York, is Judge Jesse Furman, who has repeatedly examined potential standing and jurisdictional deficiencies prior to approving data breach class action settlements. In *Cooper v. Bonobos, Inc*., 2022 WL 170622 (S.D.N.Y. Jan. 19, 2022), Judge Furman *sua sponte* ordered briefing on whether the plaintiffs had standing at the final approval stage.

The court ultimately dismissed the lawsuit, finding that the plaintiffs failed to demonstrate a sufficiently concrete risk of harm stemming from an accidental PII disclosure to establish standing. *See aff'd sub nom McMorris v. Carlos Lopez & Associates, LLC*, 995 F. 3d 295, 305 (2nd Cir. 2021). Similarly, in *In re Christie's Data Breach Litigation,* No. 24-cv-4221, 767 F. Supp. 3d 12 (S.D.N.Y. Feb. 19, 2025), Furman scrutinized whether plaintiffs had sufficiently demonstrated a risk of identity theft or fraud to establish standing.

While citing to *Gaos*, Furman requested supplemental briefing to address standing as well as fairness and structure of the proposed Settlement Agreement. *In re Christie's Data Breach Litigation*, No. 50. Judge Furman ultimately found that the plaintiffs had sufficiently pled standing and preliminarily approved the settlement.

Keep the End Game in Mind When Litigating Data Breach Class Actions

Frank v. Gaos and subsequent rulings in *Bonobos* and *Christie's* present a quandary and force resolution of certain strategic questions. Defendants who anticipate settling may question whether to raise Article III standing as a defense out of fear that it may give a court pause prior to approving a settlement.

However, doing so effectively deprives defendants of a crucial defense early on in litigation. Faced with the risk that a federal court may decide it lacks jurisdiction, some parties may instead opt for state court, either upon initial filing or removal/remand proceedings to pursue settlement approval in state court.

Forum selection has wide ranging impacts on procedural timelines, judicial experience with (and attitudes toward) class action litigation, and the likelihood of final settlement approval. Looking forward, *Gaos* places a significant burden on parties to weigh the risks of challenging standing, as dismissal could lead to subsequent litigation with potentially less favorable outcomes.

In an evolving legal landscape where federal courts may be refining standing requirements, parties must take a proactive approach to litigation strategy and settlement negotiations to anticipate obstacles and ensure the best possible resolution.

Some key take-away considerations include:

- **Forum Selection Matters**: Assess state vs. federal court based on procedural efficiencies, standing requirements, and class action settlement trends.
- **Standing Challenges Can Complicate Settlements**: Consider potential litigation risks before challenging standing, as seeking dismissal could increase legal exposure.
- **Judicial Scrutiny Varies**: Be mindful that judges may rigorously evaluate standing at final approval, potentially dismissing cases or delaying approval.
- **Settlement Timing is Key**: Weigh the benefits of settling pre-certification against the risks of standing-based dismissal.

State Court Alternatives Exist: If federal standing poses hurdles, explore options to remain in state court or dismiss in federal court to refile in state court for approval.

Judith A. Archer *and* **Sean Topping** *are partners at Norton Rose Fulbright.* **Alexis Braun** *is an associate with the firm*. **Audrey Faulks**, *a summer associate with the firm, assisted in the preparation of this articles.*

Reprinted with permission from the October 8, 2025 edition of the NEW YORK LAW JOURNAL © 2025 ALM Global Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-256-2472 or reprints@alm.com. # NYLJ-10082025-68386