
Establishing Causation and Measuring Economic Harm in Data Breach Litigation

by Hristina Bartlett; Analysis Group, Inc.

American Bar Association Antitrust Law Section (September 22, 2026)



Hristina Bartlett

A central consideration when assessing damages in data breach litigation is causation—whether and to what extent the at-issue breach caused harm to the affected individuals.¹ Although some privacy harms to consumers could be concrete and economically significant, a growing share of cyberattack-related suits involve alleged harms that are less clear-cut.

Two interrelated challenges to establishing causation emerge from an analysis of the economics of claims in data breach matters. First, the prevalence of separate cyber incidents involving the same or similar data makes it difficult to establish a causal nexus between the alleged harms and the breach at issue. Second, certain types of alleged harm, including claims of increased risk of financial fraud, may be speculative and difficult to substantiate with empirical evidence. If not addressed properly, these challenges may lead to outcomes that overstate or misrepresent consumer harm.

Ubiquity of cyber theft

Data breaches have become commonplace.² In 2025 alone, there were over 3,300 reported data compromises affecting more than 270 million individuals in the U.S.³ Of the 40 biggest data breaches in U.S. history, 15 separate breaches involved Social Security numbers, including breaches of Capital One, Equifax, and National Public Data.⁴ The Equifax breach alone involved approximately 145 million Social Security numbers, along with names, birth dates, addresses, and in some instances, driver's license numbers.⁵ Some evidence suggests that the Social Security numbers of most U.S. citizens have been compromised, with some consumers' Social Security numbers likely exposed in multiple breaches over the past decade.⁶

Data breaches of organizations are just one pathway through which bad actors can obtain information about individuals. Other methods include phishing attacks that target individuals directly and digital skimming. Phishing targeted at individuals is an online scam in which bad actors pose as a trusted source (e.g., the IRS or a bank) to induce individuals to disclose personal or financial information, while digital skimming employs malicious code injected into legitimate websites to capture payment information.⁷

Nearly half of U.S. adults surveyed by Pew Research in 2025 had experienced fraudulent charges after bad actors stole their credit or debit card information in online scams and attacks, and approximately one in four reported that they disclosed personal information in response to a scam email, text, or phone call.⁸ According to the Federal Trade Commission, "many people report giving their Social Security number and other personal information to scammers, leading to possible identity theft."⁹ Digital skimming also affected close to 11,000 unique e-commerce domains in 2024.¹⁰

Establishing causation

That the same types of data can be obtained for the same consumer through different pathways, including through multiple data breaches of unrelated companies, is highly relevant to a causation analysis.

In general, determining whether a person has suffered economic harm requires evaluating whether the alleged wrongful conduct caused the individual to be in a worse economic position than they would have been in a "but-for" world in which the alleged conduct did not occur.¹¹ This analysis requires distinguishing harm caused by the conduct at issue from harm attributable to other events or conduct. Factors that contributed to the worsening of the individual's economic position but that are unrelated to the alleged wrongful conduct must be accounted for when determining the harm attributable to that conduct.

In the context of data breach litigation, causation analysis requires considering at least two distinct questions: (1) whether the alleged harms are causally connected to the

particular information exposed in the breach at issue; and (2) what is the incremental effect, if any, of the at-issue breach, given the other pathways through which bad actors may have obtained the same or similar data for the same individuals. For example, an increase in spam messages following a data breach may be coincidental rather than causally related to the particular information exfiltrated in the breach.

But how does one isolate the effect of the at-issue data breach from unrelated cyber incidents involving the same or similar types of data? A person who experienced fraud in 2026 may have had the same data exposed in one or more prior cyber incidents, with substantial overlap in the exfiltrated information across different incidents. Attributing the harm to any single incident requires counterfactual analysis that can disentangle the economic impact of separate cyber incidents, and the data necessary for such an analysis are not always available.¹²

These causation considerations are meaningful, given that enforcement actions and class settlements resulting from data breaches impose substantial costs on companies—costs that may ultimately affect consumers through higher prices, reduced services, or diverted innovation spending.¹³

Assessing economic harm

A common theory of harm in data breach litigation is that the alleged exfiltration of personal information caused individuals to be exposed to “increased risk” by heightening the probability of future harm (e.g., identity theft or fraud) because the exfiltrated information is in the hands of bad actors.¹⁴ A central consideration in evaluating such claims is whether there is empirical support for this theory.

Allegations of future harm often assume that a data breach will result in subsequent use of the exfiltrated data by bad actors. However, exfiltration does not necessarily result in subsequent misuse. For instance, “double-extortion” ransomware attacks that involve data exfiltration as an additional bargaining chip are primarily financially motivated: The attacker’s primary objective is typically to extract payment, not to harvest and monetize consumer data.¹⁵

Consistent with this financial motivation, there is evidence that in most cases where an attacker has promised to provide a decryption key or delete stolen data, the attacker follows through on that commitment when the ransom is paid.¹⁶ Reputation creates incentives for bad actors to honor deletion commitments. This dynamic is well established in economic literature on game theory: A party whose future payoffs depend on present reputation has strong incentives to honor commitments.¹⁷ The ransomware extortion model similarly depends, at least in part, on victims believing that payment will resolve the threat. If bad actors routinely reneged on promises to delete exfiltrated data after receiving payment, future victims would be less likely to pay, and the scheme’s revenue model would deteriorate.

Helpfully, post-incident monitoring can help determine whether exfiltrated data were subsequently disseminated on the dark web. Incident-response firms, dark web monitoring specialists, and threat-intelligence analysts can track ransomware leak sites, dark web marketplaces, and other channels for evidence of whether ransomed data were actually posted, listed for sale, or otherwise disseminated. Thus, for disputes in which post-incident investigation and monitoring reveal no evidence that exfiltrated data were disseminated, sold, or misused, a claim that plaintiffs face a measurable increase in the risk of future harm requires additional empirical support. Treating every exfiltration as a de facto disclosure may overstate the injury when available evidence shows no public posting, sale, or other use occurred.

Even in cases in which exfiltrated data are posted, sold, or used, an important question is whether each person whose data were exposed faces the same level of risk of actual harm. While attackers increasingly target certain types of organizations (e.g., financial institutions or healthcare providers) because they expect to find particular types of information, they generally exfiltrate any data they can once they gain access, even though not all types of data can be used to inflict—or increase the risk of—harm. For instance, some information may already be publicly available, and not all data are “sensitive” and personally identifiable. Similarly, the data may be outdated or otherwise not useful for purposes of causing harm. The same issue may apply to hashed or encrypted data for which a plaintiff cannot show that the underlying information can be recovered or used.

More broadly, parties should exercise caution in assuming that the exfiltration or exposure of information, standing alone, results in actual harm or a measurable increase in the risk of future harm.

Relevant caselaw

Although standing and damages are distinct inquiries, case law addressing standing can illuminate a related economic question relevant to damages: When does exposure to risk become sufficiently concrete and supported to constitute cognizable harm?

Theories of economic harm in data breach cases become more complicated when different data are collected about different individuals in the same data incident. In a recent order on Defendants’ Motion to Dismiss in *In re Episource LLC Data Breach Litigation*, the district court emphasized that “the Ninth Circuit has consistently held that Article III’s requirements are satisfied before a class is certified as long as at least one named plaintiff has standing,” and that “the district court must determine that at least one named class representative has Article III standing to raise each class subclaim.”¹⁸

The requirement that there is at least one named plaintiff with standing may result in class actions with a substantial yet *unknown* share of class members who suffered no concrete harm and have no plausible risk of harm. Courts have often declined to

find Article III injury where a breach exposed only minimally sensitive or non-sensitive data and where there was no evidence that the data was targeted, actually misused, or subject to substantial risk of misuse, which are considerations that may very well apply to a majority of class members even where named plaintiffs have established Article III standing.¹⁹

The Supreme Court also recognized concerns about class members who fail to demonstrate an actual risk of harm in *TransUnion LLC v. Ramirez*, where the court held that only 1,853 of the 8,185 class members—those whose credit reports contained inaccuracies and were “concretely harmed” because their credit reports were provided to third parties—have Article III standing to seek damages in federal court.²⁰ With respect to the remaining 6,332 class members whose reports contained inaccuracies but were not shared with third parties, the court stated: “The 6,332 plaintiffs did not demonstrate that the risk of future harm materialized... Nor did those plaintiffs present evidence that the class members were independently harmed by their exposure to the risk itself.”²¹ Thus, the gap between speculative risk and demonstrated injury remains salient, not only for purposes of damages and causation analysis but also on the threshold issue of plaintiffs’ standing.

Toward a More Rigorous Approach

Data breach litigation would benefit from applying a more rigorous analysis of causation and measurement of economic harm and damages. This means that practitioners should apply the same empirical rigor to privacy damages that they would apply in any antitrust, securities, or commercial damages analysis.

Two questions may inform this analytical framework:

In a world of ubiquitous breaches, can the alleged harm be attributed to the specific at-issue incident? Damages models based on speculative attribution may face challenges under the *Daubert* or other standards governing the reliability of the expert testimony, as well as under other relevant precedent (e.g. *TransUnion*).²²

Is the alleged harm demonstrated or speculative? Alleged harms should be categorized according to their underlying empirical basis. Direct financial losses from proven identity theft related to a specific incident sit at one end of the spectrum; generalized claims of “anxiety” or “increased risk” without quantification sit at the other.

Plaintiffs should avoid relying on speculative or attenuated theories simply because they might be conceivable consequences of a data breach. Plaintiffs should also be discerning when identifying alleged harms. From the outset, they should consider whether the compromised data could plausibly produce the alleged harm and whether there is a demonstrable causal connection from the at-issue breach to that harm. Plaintiffs should also avoid defining proposed classes so broadly that they encompass individuals whose data, exposure, or circumstances do not support the asserted theory

of harm, since doing so may compound rather than resolve questions of causation and injury, as well as potentially complicating certification of the class itself under current standards.²³

Conversely, defendants should scrutinize alleged harms separately by evaluating whether the exfiltrated data could have caused each alleged injury, whether the proposed causal chain is supported by evidence, and whether alternative explanations or background risks undermine attribution to the at-issue breach. In class actions, defendants should also assess whether heterogeneity among proposed class members—including heterogeneity caused by differences in the types of data exfiltrated—undermines a common theory of harm and causation, and whether the proposed methodology establishes causation through common evidence.

Both sides would benefit from distinguishing between probability of harm, sequence of events, and causation, either in-fact or legally. That a breach *could* produce a particular harm establishes possibility; that an adverse event occurred after the breach establishes temporal sequence. However, neither establishes that the breach itself caused the event or any loss to the consumer whose data are at issue. A rigorous damages analysis will identify the evidence necessary to bridge those steps before assigning an economic value to the alleged harm.

Conclusion

In data breach litigation, there could be concerns about consumer harm from the exfiltration of personal information. However, there are challenges inherent in establishing causation and quantifying economic harm in such cases. Relevant considerations include the nature of the at-issue data, whether the alleged harm is concrete or hypothetical, and whether (and if so, how) the impact of the at-issue breach can be disentangled from that of unrelated cyber incidents involving the same data. A rigorous assessment of causation in data breach litigation requires a thorough analysis of empirical evidence related to whether the alleged harms can be attributed to the at-issue data breach and a calculation of any resulting harms grounded in evidence rather than assumptions. This approach will more properly align litigation and enforcement with the harm, if any, actually attributable to a particular data breach.

Endnotes

- 1 The causation framework described in this article should be distinguished from statutory damages frameworks that may not require the same traditional showing of causation and economic harm. The availability and scope of remedies in such frameworks depend on the governing statute and may require a different analytical approach.
- 2 See Verizon Business, *2025 Data Breach Investigations Report* (Verizon Business, 2025), 5, 68, <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>; IBM, *Cost of a Data Breach Report 2025: The AI Oversight Gap* (IBM, 2025), 4–5, <https://www.ibm.com/reports/data-breach>.
- 3 Identity Theft Resource Center, *2025 Annual Data Breach Report* (January 2026), 2–4, <https://www.idtheftcenter.org/post/2025-annual-data-breach-report-record-number-compromises/> (reporting 3,322 data compromises affecting over 270 million victims in 2025).
- 4 Kyle Chin, “Biggest Data Breaches in US History (Updated July 2026),” *UpGuard*, July 28, 2026, <https://www.upguard.com/blog/biggest-data-breaches-us>.
- 5 Kyle Chin, “Biggest Data Breaches in US History (Updated July 2026),” *UpGuard*, July 28, 2026, <https://www.upguard.com/blog/biggest-data-breaches-us>.
- 6 Suzanne Rowan Kelleher, “Everyone’s Social Security Number Has Been Compromised. Here’s How to Protect Yourself,” *Forbes*, August 1, 2019, <https://www.forbes.com/sites/suzannerowankelleher/2019/08/01/everyones-social-security-number-has-been-compromised-heres-how-to-protect-yourself/>; Kyle Chin, “Biggest Data Breaches in US History (Updated July 2026),” *UpGuard*, July 28, 2026, <https://www.upguard.com/blog/biggest-data-breaches-us>; “Identity Theft Resource Center 2025 Annual Data Breach Report: Record Number of Data Compromises in 2025; 79 Percent Jump Over Five Years,” *Identity Theft Resource Center*, January 29, 2026, <https://www.idtheftcenter.org/post/2025-annual-data-breach-report-record-number-compromises/>; Identity Theft Resource Center, *2025 Annual Data Breach Report* (January 2026), 8, 29 (reporting that of the 3,322 data compromises in 2025, 2,243 involved SSNs).
- 7 See, e.g., “Phishing Scams,” Federal Trade Commission, accessed September 4, 2026, <https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams>; “E-Skimming,” Florida Department of Agriculture and Consumer Services, accessed September 4, 2026, <https://www.fdacs.gov/Consumer-Resources/Scams-and-Fraud/E-Skimming>. Phishing has consistently been the most reported type of internet crime to the FBI, with nearly 200,000 complaints in both 2024 and 2025. Federal Bureau of Investigation, Internet Crime Complaint Center, *2024 Internet Crime Report* (Washington, DC: Federal Bureau of Investigation, 2025), 9, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf; Federal Bureau of Investigation, Internet Crime Complaint Center, *2025 Internet Crime Report* (Federal Bureau of Investigation, 2026), 7, https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.
- 8 Jeffrey Gottfried, Eugenie Park, and Monica Anderson, “Online Scams and Attacks in America Today,” *Pew Research Center*, July 31, 2025, <https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/>.
- 9 Emma Fletcher, “IYKYK: The Top Text Scams of 2022,” *Federal Trade Commission*, June 8, 2023, <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022>.
- 10 Recorded Future Insikt Group, *Annual Payment Fraud Intelligence Report: 2024* (Recorded Future, January 21, 2025), 6, <https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-2025-0121.pdf>; Fayyaz Makhani, “How to Spot and Stop E-Skimming Before It Hijacks Your Customers—and Your Credibility,” *VikingCloud*, June 24, 2025, <https://www.vikingcloud.com/blog/how-to-spot-and-stop-e-skimming-before-it-hijacks-your-customers-and-your-credibility>.
- 11 See, e.g., National Academies of Sciences, Engineering, and Medicine and Federal Judicial Center, *Reference Manual on Scientific Evidence*, 4th ed. (National Academies Press, 2025), 754–756, <https://doi.org/10.17226/26919>.
- 12 See, e.g., *In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 626 F. Supp. 3d 814 (D. Md. 2022).
- 13 IBM, *Cost of a Data Breach Report 2025: The AI Oversight Gap* (IBM, 2025), 41, <https://www.ibm.com/reports/data-breach>; Chris Zhijian He et al., “The Impact of Reported Cybersecurity Breaches on Firm Innovation,” *Journal of Information Systems* 34, no. 2 (2020): 190.
- 14 See Daniel J. Solove & Danielle Keats Citron, “Risk and Anxiety: A Theory of Data-Breach Harms,” *Texas Law Review* 96, (2018): 737.

- 15 “What Is Double Extortion Ransomware?,” SentinelOne, last modified August 11, 2025, <https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-double-extortion/>.
- 16 Palo Alto Networks, *Unit 42 Global Incident Response Report 2026* (2026), 27, <https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report>.
- 17 See, e.g., Thomas C. Schelling, *The Strategy of Conflict* (Harvard University Press, 1960), 42–46, 60; Lillian Ablon et al., *Markets for Cybercrime Tools and Stolen Data*, (RAND Corporation, 2014), 6; Terrence August et al., “Economics of Ransomware: Risk Interdependence and Large-Scale Attacks,” *Management Science* 68, no. 12 (2022): 8997, 8999.
- 18 *In re Episource LLC Data Breach Litig.*, No. 2:25-cv-05330-SB-MBK, 2026 U.S. Dist. LEXIS 165465, at *14-15 (C.D. Cal. July 13, 2026) (internal quotations omitted).
- 19 *McMorris v. Carlos Lopez & Assoc., LLC*, 995 F.3d 295, 301–03 (2d Cir. 2021); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1343–45 (11th Cir. 2021); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42–46 (3d Cir. 2011); *Chambliss v. CareFirst, Inc.*, 189 F. Supp. 3d 564, 570–71 (D. Md. 2016); *Khan v. Children’s Nat’l Health Sys.*, 188 F. Supp. 3d 524, 531–33 (D. Md. 2016); *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431, 435–39 (2021); *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259, 1273–77 (11th Cir. 2019).
- 20 *TransUnion LLC v. Ramirez*, 594 U.S. 413, 417 (2021).
- 21 *TransUnion LLC v. Ramirez*, 594 U.S. 413, 437 (2021).
- 22 See *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993); *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021).
- 23 See, e.g., *Comcast Corp. v. Behrend*, 569 U.S. 27 (2013).

Published by the American Bar Association ©2026. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.