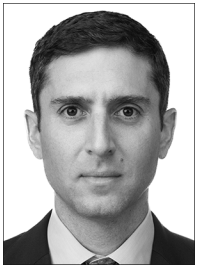
Using the Dark Web to Defend Data Breach Class Actions

Scott J. Hyman, Genevieve Walser-Jolly, Lela Ames, Jack Altura, & TaeVeon Le

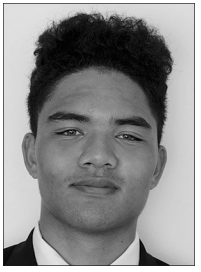
Scott J. Hyman

Genevieve Walser-Jolly

Lela Ames



Jack Altura



TaeVeon Le

Scott J. Hyman is a Partner with Womble Bond Dickinson (US) LLP in Orange County, California, and has devoted over 30 years of practice to representing the financial services industry in compliance, risk management, litigation, and cybersecurity. Scott holds CIPP (US and EU), CIPM, and CIPT credentials with the International Association of Privacy Professionals. Scott is a Vice President of the Conference on Consumer Finance Law.

Genevieve Walser-Jolly is a Partner with Womble Bond Dickinson (US) LLP in Orange County, California, and represents financial institutions, including banks, lenders, and loan servicers. Her practice includes defending individual and consumer class actions (for example, data privacy, mortgage servicing, TCPA, and auto finance). Genevieve helps clients (in and outside of financial services) set up data privacy and security programs to comply with federal statutory schemes and the evolving patch-

work of state privacy laws. Genevieve is a Vice President of the Conference on Consumer Finance Law.

Lela Ames is a Partner in Womble Bond Dickinson (US) LLP's Washington D.C. office. Lela is a versatile, trial-tested litigator, having served as lead counsel and trial counsel in a wide range of disputes involving data breach class actions, financial services, manufacturing, contracts, and business torts.

Jack Altura is an Associate with Womble Bond Dickinson (US) LLP in Orange County, California, and is a member of Womble's business litigation practice group. Mr. Altura focuses his practice on complex business litigation, class action defense, and data privacy and cybersecurity litigation. He advises clients in multidistrict litigation, class actions, and single-plaintiff claims, as well as assists clients responding to civil investigative demands from state attorneys general and federal agencies.

TaeVeon Le is a law student at the University of San Francisco School of Law and a candidate to receive his Juris Doctor with the class of 2028. Tae received his Bachelor of Arts in International Relations with the double minors in History and in French from the Leland Stanford Junior University, where he was also a member of Stanford's Varsity Football Team. Tae received his Master of Arts Degree in Conflict, Security, and Development from The Kings College, London, England, where he also was a war games facilitator for NATO and worked for the United Kingdom Ministry of Defence.

I. Contents

II. Introduction

"There are only two types of companies: Those that have been hacked and those that will be hacked."[1] "Cybercriminals who steal data are primarily suppliers responding to strong demand, sometimes even for their own use, but more often to turn a profit. Individuals and organizations pay handsomely for some good old stolen information."[2] But the opposite side of that coin may also be true. Namely, there are only two types of data: data that has been compromised multiple times and data that will be compromised multiple times.

Data breach litigation is maturing as it evolves in response to the increasing frequency and complexity of data breaches. The number of data breach class action cases filed has multiplied, in part attributable to court decisions that have made it easier for plaintiffs to show standing and to prove causation. There is a growing trend of litigation related to data breaches, alongside official regulatory actions, and evolving into data scraping and non-breach privacy litigation.

The character of data breaches, both in size and complexity, has evolved. Financial services, healthcare, and professional services were the three industry sectors that recorded the most data breaches.[3]

> In 2023, data breaches rose by 72% compared to 2022, but the number of victims declined, with approximately 353 million individuals affected. However, 2024 saw a dramatic shift—the total number of breaches remained high, but the number of victims skyrocketed by 312%. One major differentiator was the increasing scale of mega-breaches. In 2023, many incidents remained isolated within single organizations, but in 2024, entire supply chains and interconnected digital ecosystems were impacted. Attackers leveraged vulnerabilities in third-party services, leading to widespread data exposure.[4]
>
> Defense spending and the expected number of class actions hit a new record for 2024, accounting for a tenth straight year of growth. Spending

1. Stephen Barnes, *There Are Two Types of Companies: Those Who Know They've Been Hacked & Those Who Don't*, Dynamic Bus. (Mar. 29, 2018), https://dynamicbusiness.com/locked/there-are-two-types-of-companies-those-who-know-theyve-been-hacked-those-who-dont.html (quoting Robert S. Mueller, III, former Director of the FBI and Special Counsel into the Russian interference of the U.S. election).
2. David Soffer, *The Dark Web's Currency of Choice: Stolen Data*, It Sec. Guru (June 6, 2025) https://www.itsecurityguru.org/2025/06/02/dark-webs-currency-choice-stolen-data/.
3. *Number of Data Compromises and Individuals Impacted in the United States from 2021 to 2025*, Statista (Feb. 15, 2026), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
4. *The 2024 ITRC Data Breach Report: Record-Breaking Breaches and What Comes Next*, Bluefin (Feb. 5, 2025), https://www.bluefin.com/bluefin-news/2024-itrc-data-breach-report-record-breaking-breaches/.

> on class actions by the reporting companies came to about $4.21 billion for 2024. This $4.21 billion number was a 12.3% increase from the prior year, amounting to a $300 million increase. However, the defense spending takes on another level of appreciation when it is calculated in connection with corporate litigation budgets. Spending on class actions in 2024 accounted for 12.5% of corporate litigation budgets. This increased spending also translated into an interesting increase in in-house counsel time taken to manage these cases, usually with outside law firms. The 2025 survey shows that class actions added the equivalent of one additional workday per week to in-house attorneys' management responsibilities for purposes of defending these matters.[5]

"Two-thirds of corporate counsel participating in the survey expected new class actions to arise after the use of generative AI. One president and CEO of a large technology company said, '[g]enerative AI, data breaches, and privacy are the new frontier.'"[6] The data bears this out, in multiples. "[M]ore than half (61%) of U.S. adults report receiving notice that their personal data was compromised—with 44% noting their personal data has been compromised *multiple* times."[7]

> [T]he number of sets of PII [personal identifying information] that belong to U.S. persons and are exposed in breaches each year has consistently exceeded the total U.S. adult population, often several times over. This seemingly nonsensical statistic indicates that hundreds of millions of Americans have had their PII stolen over and over again, often multiple times each year.[8]

A company-focused analysis, however, tells only half the story about the maturation of data breach litigation. It is self-evident that, from a data-subject standpoint, receipt of multiple data-breach notices has become commonplace and part of modern digital life.[9] It is not uncommon for individ-

5. W. Michael Hensley, *Recent Survey Shows Class Actions on the Rise and More Expensive to Defend*, FBT Gibbons (Apr. 9, 2025), https://fbtgibbons.com/recent-survey-shows-class-actions-on-the-rise-and-more-expensive-to-defend/.
6. *Id.*
7. Sarah Pike, *U.S. News 360 Reviews Survey Reveals Americans' Data Breach Experience, Cyber Attack Fears*, U.S. News & World Rep. (Jan. 24, 2024), https://www.usnews.com/press-room/consumer-insights-studies/2024-01-24/u-s-news-360-reviews-survey-reveals-americans-data-breach-experiences-cyber-attack-fears (emphasis in original).
8. Jordan Hefcart, *Economic Justice via Public Insurance: What Data Breach Law Can Learn from Pandemics and Worker Injuries*, 113 Cal. L. Rev. 2047, 2054 (2025).
9. Ann Carrns, *What to Do if You're a Data Breach Victim (and You Probably Are)*, Seattle Times (Apr. 5, 2026, 6:00 AM), https://www.seattletimes.com/business/what-to-do-if-youre-a-data-breach-victim-and-you-probably-are/ ("Do you feel that you get an awful lot of data breach notices in the mail? You're not alone. In a 2025 survey of 1,040 people by the Identity Theft Resource Center, a nonprofit that tracks breaches and advises victims, 80 percent said they had received at least one breach notice in the previous 12 months. About 40 percent

uals to receive multiple notifications from different entities about data breaches, such as banks, medical clinics, and data aggregators.

Thus, too, must the analysis of data subjects' standing in class action litigation evolve to recognize the effect of multiple data breaches on a particular data subject. "Article III standing can be an uphill battle for data-breach plaintiffs, who must allege a 'concrete harm,' not just an 'asserted risk of future harm.'"[10]

> A successful defense often focuses on 'breaking the chain' of causation. If a user's data was already available on the dark web due to five other prior breaches, it becomes difficult for the plaintiff to prove that this specific breach caused their identity theft. Forensic data 'fingerprinting' is now a standard tool used in 2026 to defend against broad corporate liability claims.[11]

This defense is not dependent on whether the "new" data from the data breach at issue was posted on the dark web or not—although such posting or non-posting is relevant to the standing analysis in and of itself.[12]

This article explores a data-centric and data subject-centric evaluation of the effects of multiple-compromised data and data subjects on data breach class action litigation.[13]

---

said they had received three to five separate notices. The findings ring true to me.").

10. Flores v. Computer Merch., Ltd., No. 25-CV-00038-AJB-DEB, 2026 WL 457566, at *11 (S.D. Cal. Feb. 18, 2026) (quoting TransUnion LLC v. Ramirez, 594 U.S. 413, 437 (2021)) (citing *In re* Cal. Pizza Kitchen Data Breach Litig., 129 F.4th 667, 678 (9th Cir. 2025)).

11. *International Data Breach Class Action: Legal Liability and Cross-Border Risk*, SJKP Law Firm LLP (Feb. 8, 2026), https://www.daeryunlaw.com/us/practices/detail/international-data-breach-class-action.

12. Arianna C. Goldstein, *An Update as to Standing in Data Breach Class Actions*, Baird Holm LLP (Nov. 21, 2025), https://www.bairdholm.com/blog/an-update-as-to-standing-in-data-breach-class-actions/ (citing Holmes v. Elephant Ins. Co., 156 F.4th 413, 428–35 (4th Cir. 2025)) ("The Court held that publication of a driver's license number on the dark web is public exposure of sensitive, tightly controlled information. This is closely related to the harm addressed by the tort of public disclosure. The court held that a driver's license number is private information even though: a driver's license number per se is not embarrassing, Elephant did not affirmatively disclose it, and the dark web is not a traditional 'public' forum. Thus, sensitive information published on the dark web is concrete injury. And, because this injury was actual and concrete, Cardenas and Holmes have standing and can pursue damages. Two plaintiffs, Shaw and Bias, lacked standing entirely, because they did not allege that their stolen information was publicly accessible on the dark web or misused. Those plaintiffs whose numbers were compromised, but not shown to be publicized or posted on the dark web, did not have standing. None of the plaintiffs have standing to seek injunctive or declaratory relief, because they failed to show any imminent future harm.").

13. A truncated, companion article can be found at Hyman, et. al., *The Dark*

III. Proving that Data Breach Victims Were Subject to Multiple Prior Data Breaches

A. What is the Dark Web?

> The term "dark web" is widely used, but not always accurately. To clarify, the Internet is generally divided into three layers: **Surface web:** the most visible and easily accessible part of the Internet. These are the websites we use every day. **Deep web:** content that's not indexed by search engines and requires special access or authorization to view. This layer is estimated to comprise about 95% of the entire Internet. **Dark web:** a subsection of the deep web. Around 50% of dark web content is thought to be illegal. It's a hub for criminal activity, including the sale of stolen data. The dark web offers near-total anonymity. Accessing specific content, such as platforms selling personal data, typically requires an invitation or prior access. This hidden, anonymous nature makes the dark web ideal for fast, discreet criminal transactions.[14]

The dark web is a "section" of the internet that can be accessed with dark web browsers. Tor, a dark web browser, obfuscates the origin of user traffic by essentially "bouncing" requests through an intentionally complex series of intermediate relays, of which there could be thousands. Decentralization of devices that relay data makes it extremely difficult to track a digital trail. Websites on the dark web exist on this encrypted network, just as they do on the conventional internet. But traditional search engines cannot find them, and that makes the dark web anonymous and untraceable—factors tailor-made for a digital marketplace of illicit trading where malicious actors usually will peddle stolen data.[15] The dark web is an expansive community, with over 65,000 ".onion" URLs existing on the Tor network

Web and Traceability in Data Breach Class Actions, ___ The Review of Banking & Financial Services ___ (forthcoming 2026) (on file with author).

14. Robert Simpson, *The Link Between Data Breaches and the Dark Web Explained*, EdTechRCE https://edtechrce.org/the-link-between-data-breaches-and-the-dark-web-explained/; *see also* Fero v. Excellus Health Plan, Inc., 304 F. Supp. 3d 333, 342 (W.D.N.Y. 2018), *order clarified*, 502 F. Supp. 3d 724 (W.D.N.Y. 2020) ("According to [plaintiffs' expert] Jones, 'the Deep Web is the portion of the internet that is not indexed by standard search engines,' while 'the Dark Web is a subset of the Deep Web, and consists of sites that are inaccessible to most users, often requiring specialized encryption software and other tools that mask the locations and identities of their users.' Jones further states that 'the Deep and Dark Web are commonly used for criminal activity' and 'the sale and purchase of PII and PHI compromised in a data breach.'" (citation modified)).

15. Robert Elgart, *The Data Black Market: Where Hackers Take Stolen Data*, Turn-Key Techs. (Aug. 5, 2019), https://www.turn-keytechnologies.com/blog/article/the-data-black-market-where-hackers-take-stolen-data/ (noting this speed is particularly relevant for credit card theft).

alone. The nature of these sites varies, from chat rooms and forums to the marketplaces that society has come to associate with the community.[16]

> While some use the dark web for privacy and free speech purposes, its characteristic anonymity has also attracted cybercriminals and other malicious actors who carry out illicit activities online. Many illegal goods and services are bought and sold on the dark web, including stolen financial information, counterfeit money, weapons, malware, hacked accounts and drugs. These so-called darknet transactions often involve cryptocurrencies like **bitcoin** to further obscure users' identities.[17]
>
> Tor ensures your privacy by encrypting your internet traffic in multiple layers, much like peeling an onion (hence the name). When your data is sent through the Tor network, it passes through at least three nodes—a guard node, a middle node, and an exit node. Each node only knows the immediate source and destination of the data but not the entire path, making it incredibly challenging to trace the data back to you.[18]

"The dark web is a subset of the deep web that is intentionally hidden, requiring a specific browser—Tor—to access, as explained below. No one really knows the size of the dark web, but most estimates put it at around 5% of the total internet."[19] Accessing the dark web requires using an an-

16. Aditi Kumar & Eric Rosenbach, *The Truth About the Dark Web*, Fin. & Dev., Sept. 2019, at 22, https://www.imf.org/-/media/files/publications/fandd/article/2019/september/the-truth-about-the-dark-web-kumar.pdf ("Today, over 65,000 unique URLs ending with .onion exist on the Tor network. A 2018 study by computer security firm Hyperion Gray catalogued about 10 percent of these sites and found that the most prevalent functions facilitate communication via forums, chat rooms, and file and image hosts, as well as commerce via marketplaces.").

17. Gabriel O. Rodriguez Cruz, *What to Do if Your Information Is Found on the Dark Web*, Money (Feb. 26, 2025), https://money.com/what-to-do-if-your-information-is-found-on-the-dark-web/; Sharon D. Nelson, Esq., & John W. Simek, *Ashley Madison and the Deep (and Sometimes Dark) Web*, Ass'n of Internet Research Specialists (Nov. 2015), https://aofirs.org/wp-content/uploads/2018/08/Ashley-Madison-and-the-Deep-Web.pdf ("Much of the Deep Web is perfectly legitimate. Many privacy advocates are there, wishing to operate without being tracked. Journalists are often there, generally concerned about government prying. You can also find whistleblowing sites. Some of it is also dynamically generated web pages or forums which require registration. We're not sure how much of the Deep Web is also the Dark Web, though experts say it is a small percentage. The Dark Web contains the seamy places where drugs and guns are sold, human trafficking occurs, criminals offer their services for hire, hackers and cybercriminals operate and child porn is viewed, distributed, and sold. And those are only some of the activities on the Dark Web.").

18. *What is Tor?*, Lenovo, https://www.lenovo.com/us/en/glossary/tor/?orgRef=https%253A%252F%252Fwww.google.com%252F&srsltid=AfmBOoorZV8vdIbd5VTwzZunXPdbTeXSlslWOCQO6y11BesKK23MNAX-.

19. Darren Guccione, *What Is the Dark Web? How to Access It and What You'll Find*, CSO (Apr. 2, 2024), https://www.csoonline.com/article/564313/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.

onymizing browser called Tor. The Tor Browser routes your web page requests through a series of proxy servers operated by thousands of volunteers around the globe, rendering your IP address unidentifiable and untraceable. Tor works like magic, but the result is an experience that's like the dark web itself: unpredictable, unreliable, and maddeningly slow.

> The dark web is notorious as a hub for illegal activities, particularly the trade of stolen data for a price. It's a covert marketplace where cybercriminals can anonymously buy and sell leaked credentials and other sensitive information. These transactions perpetuate and escalate cybercrimes, establishing a continuous cycle. Getting a handle on the complexities of dark web market operations is crucial for a comprehensive understanding of the stolen data lifecycle.[20]
>
> Once harvested, the data is cleaned, categorized, and auctioned like inventory in a wholesale warehouse. A full identity—known as "fullz"—can fetch between $10 and $100 depending on its quality. A hacked bank account with a clean transaction history? That can go for hundreds. Here's how the monetization lifecycle works: **Bundling and Valuation:** Cybercriminals compile stolen data into categories like login credentials, medical records, tax IDs, or passport scans. Each bundle is priced based on its utility and rarity. **Dark Web Marketplaces:** Platforms like Genesis, BlackForums, and Hydra function like eBay—complete with user reviews, refund policies, and customer service. Sellers build reputations over time, and the most reliable vendors command premium prices. **Crypto-Powered Transactions:** Payments are made via cryptocurrencies such as Bitcoin and Monero to maintain anonymity. Smart contracts and escrow services often protect both parties. **Exploitation and Resale:** Buyers may directly use the data to commit fraud—applying for loans, stealing medical benefits, or launching phishing campaigns—or they may resell the information to other actors.[21]

While Bitcoin still remains the principal coin of commerce in the dark web, criminals have begun to use alternatives like Monero in response to the success of the authorities in tracking criminals through the Bitcoin blockchain.[22]

---

20. *Data Breaches and the Dark Web: Protect Your Organization*, Proficio (Apr. 23, 2024), https://www.proficio.com/data-breaches-and-the-dark-web/.
21. Ankit Sharma, *Dark Web Threats*: *How Your Data Is Compromised and Monetized by Cybercriminals*, Cyber Def. Mag. (June 4, 2025), https://www.cyberdefensemagazine.com/dark-web-threats-how-your-data-is-compromised-and-monetized-by-cybercriminals/; *see also* Justyn Newman, *The Digital Black Market: How Your Data Is Bought, Sold, and Traded After a Breach*, PC Mag (Sept. 29, 2025), https://www.pcmag.com/explainers/the-digital-black-market-how-your-data-is-bought-sold-and-traded-after ("The hackers or attackers responsible for the breach typically aren't the ones who end up using your data. Think of it like a luxury jewelry store robbery: The thieves aren't stealing the items to wear them—they're after the profit they can make by selling them to others. Similarly, your data is just a valuable asset in an underground marketplace.").
22. Mohammed Khalil, *How Law Enforcement Tracks Criminals on the Dark Web: Techniques, Tools, & Case Studies*, Deepstrike (Nov. 16, 2025), https://deep-

B. What Data does the Dark Web Hold Regarding Prior Data Breaches?

The dark web offers a marketplace for the purchase of credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials, software that helps hack into other people's computers, login credentials to bank accounts, counterfeit currency, prepaid debit cards, or a "lifetime" Netflix premium account.[23] The marketplace also offers hackers-for-hire to attack computers or "ransomware-as-a-service" (RaaS).[24] Dark web commerce sites have the same features as any e-retail operation, including ratings/reviews, shopping carts, and forums, but there are important differences. One is quality control. When both buyers and sellers are anonymous, the credibility of any ratings system is dubious. Ratings are easily manipulated, and even sellers with long track records have been known to suddenly disappear with their customers' crypto-coins, only to set up shop later under a different alias.

As in the real world, the price one pays for stolen data fluctuates as the market changes. According to Privacy Affair's Dark Web Price Index 2021, these are the most current prices for some of the data and services commonly traded over the dark web: $25–$35 for a cloned credit card with PIN; $240 for credit card details with account balance up to $5,000; $120 for stolen online banking logins with at least $2,000 in the account; $50–$340 for PayPal transfers from stolen accounts; $610 for hacked Coinbase verified account; $1–$60 for a hacked social media account; $80 for a hacked Gmail account; $1,000 for a hacked eBay account with good reputation.[25] Since 2021, these prices have decreased over the years, some being cut in half, for example, credit card details with an account balance of up to $5,000 costing only $110 in 2023.[26]

---

strike.io/blog/how-law-enforcement-tracks-criminals-on-the-dark-web ("Of course, criminals adapt[;] many now use coins like **Monero** or **mixers/tumblers** to obscure their trails.").

23. Guccione, *supra* note 19.

24. Soham Halder & Atchutanna Subodh, *What Is Ransomware-as-a-Service (RaaS)? How Cybercrime Became a Business Model*, Analytics Insight (Dec. 9, 2025), https://www.analyticsinsight.net/cybersecurity/what-is-ransomware-as-a-service-raas-how-cybercrime-became-a-business-model ("Ransomware-as-a-Service is a model where cybercriminals develop ransomware tools and sell them to affiliates. Attackers buy these packages on the dark web. These include dashboards, encryption tools, automation scripts, and detailed guides. RaaS platforms are almost similar to the SaaS products. It may offer subscription plans, one-time purchases, and revenue-sharing models. This structure helps developers make a profit without launching attacks. It led to the formation of a profitable nexus of criminal activities that anyone could join.").

25. Guccione, *supra* note 19.

26. Miklos Zoltan, *Dark Web Price Index 2023*, PrivacyAffairs.com (Apr. 23, 2023), https://www.privacyaffairs.com/dark-web-price-index-2023/.

C. How to Get Information from the Dark Web.

It is true that some "do-it-yourself" tools exist to scan the Dark Web.[27] But in high-stakes data breach litigation, a more formal approach should be employed, notwithstanding the extra cost. The best way to obtain data from the dark web for purposes of litigation is to hire forensic experts.[28] This ensures the investigation will be protected by the attorney-work product doctrine. At a minimum, "[e]arly expert involvement matters in data breach litigation because technical findings often shape allegations, discovery, and damages."[29]

Alternatively, if the expert intends to testify and the information is to be used in litigation, guidelines can be put in place to address admissibility concerns regarding the information. Courts have relied on dark web scrubs

27. Abeerah Hashim, *Proton's Dark Web Tool Exposes Data Breaches First*, PrivacySavvy (Oct. 30, 2025), https://privacysavvy.com/news/cybersecurity/proton-launches-dark-web-patrol-to-expose-data-breaches/ ("Proton's new Data Breach Observatory will actively scan the dark web for stolen customer data being sold by hackers."); Cecilia Garzella, *The Database You Don't Want to Need: Check to See if Your Health Data Was Hacked*, Usa Today (Apr. 9, 2024, 12:35 PM), https://www.usatoday.com/story/news/investigations/2024/04/09/how-to-check-health-care-data-breaches/73219266007/.

28. *See Dark Web Investigation*, Forensicss Cybersecurity Investigator, https://forensicss.com/dark-web-investigation/ ("A Dark Web Data Leaked Investigation identifies if your sensitive data—such as emails, passwords, financial records, or customer files—has been exposed or sold on hidden online marketplaces. Our analysts use proprietary tools to monitor dark web forums and breach dumps to verify exposure and assess the risks."); *Dark Web Investigations—Get Answers from Our Consultants*, Corp. Investigation Consulting, https://corporateinvestigation.com/digital-forensics/dark-web-investigations/ ("Corporate Investigation Consulting's digital forensics team can discreetly and effectively investigate dark web activities. We leverage cutting-edge techniques and in-depth knowledge to conduct criminal investigations, uncover evidence, identify perpetrators, and mitigate potential damage to your organization. In the murky depths of the dark web, threats to your corporation can proliferate unseen. From the sale of stolen data and intellectual property to the planning of ransomware attacks and other illicit activities, the risks are significant and demand an experienced partner."); *A Class Above: Expert Support for Data Breach Class Action Defense*, Cybereason, https://www.cybereason.com/blog/expert-support-class-action ("Cybereason's threat intelligence and dark web analysis team plays a vital role here by: Determining if stolen data was already present on the dark web from a prior breach, Confirming whether the data has been sold, posted, or misused, Analyzing whether the type of data (e.g., hashed credentials, PII, internal documents) is of actual value to cybercriminals") (A Class Above: Expert Support for Data Breach Class Action Defense).

29. Hall v. Healthcare Servs. Grp. Inc., No. 2:25-cv-04908-JDW, 2025 WL 3280943, at *2 (E.D. Pa. Nov. 24, 2025).

from forensic experts,[30] sometimes to demonstrate that the allegedly exfiltrated data was *not* on the dark web.[31] Although some of the forensic expert's testimony would be percipient, it should be anticipated that their testimony will be subject to the usual evidentiary rules of foundation and for admitting expert testimony.[32] The Court of Appeals for the Ninth Circuit

30. *In re* Mednax Servs., Inc., Customer Data Sec. Breach Litig., 603 F. Supp. 3d 1183, 1206 (S.D. Fla. 2022) ("In support of these arguments, Defendants cite the findings of their experts: Austin Berglas, who led a team of analysts that scoured the dark web to investigate the veracity of these Plaintiffs' allegations, and Kathleen O'Hara, who conducted an exhaustive search of all locations where Mednax would expect Social Security numbers to be located. Because this is a factual challenge, the Court may consider these experts' declarations even though they are presented outside the pleadings." (citation modified)); *In re* Flagstar Dec. 2021 Data Sec. Incident Litig., No. 22-cv-11385, 2024 WL 5659583, at *2 (E.D. Mich. Sept. 30, 2024) ("Flagstar hired two cybersecurity vendors to monitor the dark web in October 2022 and found no evidence that the [cyber attackers] released any Flagstar data from this data breach. However, some of named Plaintiffs' data was located on the dark web. According to one of Flagstar's cybersecurity experts, this was 'data from the Accellion Incident'—a breach Flagstar customers had been compromised in when a ransomware gang targeted the servers of Accellion (a vendor Flagstar used)." (citation modified)).

31. Podroykin v. Am. Armed Forces Mut. Aid Ass'n, 634 F. Supp. 3d 265, 268 n.1 (E.D. Va. 2022) ("Defendant disputes [the fact that data taken through ransomware was placed on the dark web]. To do so, defendant offers a declaration by William Hardin, a purported expert in information technology, digital forensics, and cyber extortion. Hardin's declaration states that, based on searches of the dark web, none of the information from the January 2021 attack was posted on the dark web. *See* Declaration of William Hardin (Dkt. 39-1). Because, on a Rule 12(b)(1) challenge to standing, 'the district court is entitled to decide disputed issues of fact with respect to subject matter jurisdiction,' *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009), it is appropriate to consider the declaration. But as discussed *infra*, whether plaintiff's information was ever on the dark web is not material to the resolution of this Motion. This is so because, regardless of whether plaintiff's PII was on the dark web, plaintiff concedes that it is no longer there, as DarkSide's websites were shut down at least 16 months ago. Thus, for reasons that follow *infra*, plaintiff's claim to standing is too attenuated."); *see also* Kate Fazzini, *Equifax Mystery: Where Is the Data?*, CNBC (Feb. 13, 2019), https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html [https://perma.cc/FDG4-FBMC] (security experts had not been able to locate the Equifax data for sale on the dark web post-breach for use in typical identity theft schemes).

32. *The Evidentiary Weight of Cyber Forensics from the Dark Web: Admissibility and Relevance to Bank Secrecy Act Compliance: Executive Summary and Strategic Overview*, SCRIBD, https://www.scribd.com/document/959137417/Dark-Web-Forensics-and-BSA-Admissibility ("The proliferation of illicit activity on the Dark Web, facilitated by anonymity networks such as Tor and the widespread use of convertible virtual currencies (CVCs), presents complex challenges for

has held that such expert testimony should be admissible in the aid of the jury.[33]

IV. Judicial Treatment of Multiple-Compromised Data Subjects' Prior Breach History

A. Traceability as a Function of Article III Standing.

"To establish the individual standing prerequisites, a plaintiff must have '(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.'"[34] To satisfy Article III standing, a plaintiff must allege an injury in fact that is "fairly traceable to the challenged action of the defendant," requiring a "causal connection between the injury and the conduct complained of."[35] "[A] claim for damages requires a concrete harm that has in fact occurred."[36] Data subjects whose data has been the subject of multiple compromises face challenges in demonstrating traceability.

Courts have taken different approaches in evaluating traceability at the pleading stage. Some courts found traceability to be resolvable at the pleadings stage.[37]

---

both law enforcement and financial institutions governed by the Bank Secrecy Act (BSA). The evidentiary value of digital artifacts recovered from this environment is critically high, as these artifacts often serve as the only reliable linkage between anonymous criminal conduct and identifiable perpetrators or regulated financial channels. However, the legal admissibility of Dark Web forensic evidence is not guaranteed. It is contingent upon a hyper-rigorous adherence to established legal standards—specifically, the principles of integrity, authenticity, and an unbroken Chain of Custody (COC). Furthermore, the complexity inherent in tracing encrypted communications and de-anonymizing cryptocurrency transactions requires expert testimony that reliably satisfies the Daubert standard for scientific evidence.").

33. United States v. Saini, 23 F.4th 1155, 1166 (9th Cir. 2022) ("Inspector Shen's [expert] testimony mainly focused on details about *how* thieves obtain personal information and use such information to commit fraud. For example, he explained that thieves can easily obtain personal information on the dark web and described how that information can then be used to gain access to credit card accounts. The district court reasonably concluded that these types of details would help the jury, and thus the court properly admitted Inspector Shen's testimony under Rule 702(a).").

34. Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016).

35. *In re Mednax Servs., Inc.*, 603 F. Supp. 3d at 1203 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).

36. Dinerstein v. Google, LLC, 73 F.4th 502, 512 (7th Cir. 2023) (citing *Ramirez*, 594 U.S. at 435–37); *see also* Pierre v. Midland Credit Mgmt., Inc., 29 F.4th 934, 938 (7th Cir. 2022) ("A plaintiff seeking money damages has standing to sue in federal court only for harms that have in fact materialized.").

37. Andrew Serwin et al., *The Dark Web—The Next Frontier in Data Breach Standing Analysis amid a Deepening Circuit Split*, Bloomberg L. (Mar. 9, 2018, 1:02

Courts have dismissed data breach claims where the alleged harms were not fairly traceable to the breach . . . even where plaintiffs claimed their personally identifiable information was found on the dark web, if the complaint did not plausibly allege that such misuse was linked to the defendant's breach.[38]

PM), https://news.bloomberglaw.com/privacy-and-data-security/the-dark-web-the-next-frontier-in-data-breach-standing-analysis-amid-a-deepening-circuit-split ("Moreover, [*Fero*] is notable in that it relies on extrinsic evidence—Dark Web searches and a forensic report—to reach a conclusion that appears to be inconsistent with the conclusions of *Clapper.* In particular, the court finds standing in the absence of evidence that the alleged breach at issue (as opposed to a different breach) was the source of the information that was allegedly for sale on the Dark Web. Finally, *Fero* raises questions about whether reliance on extrinsic evidence is—or should be—an approach courts adopt in addressing standing at the motion to dismiss stage where the evidentiary record is incomplete, and whether forensic reports and investigations prepared in the wake of data breaches may increasingly be subject to discovery. Whether the use of Dark Web searches and reliance upon forensic reports at the pleading stage becomes more common remains to be seen, but the case is one to watch." (first citing Fero v. Excellus Health Plan, Inc., 304 F. Supp. 3d 333 (W.D.N.Y. 2018); and then citing Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013)).

38. Raika Casey & Alexis Opper, *Courts Are Still Willing to Dismiss Data Breach Lawsuits for Lack of Standing*, JD Supra (Mar. 11, 2025), https://www.jdsupra.com/legalnews/courts-are-still-willing-to-dismiss-2003796/. *See also* Midkiff v. Shoe Show, Inc., Case No. 1:24-cv-858, 2026 WL 880210 (M.D.N.C. March 30, 2026) ("It appears to this Court that the Fourth Circuit's opinion in Holmes does not substantially change the legal framework previously set out in Beck and Hutton. Holmes cites approvingly to, and relies upon, both cases in its analysis. *See* 156 F.4th at 429 n.18, 430–32. Beck, Hutton, and Holmes appear to cumulatively hold the following. A data breach plaintiff must allege more than the mere fact of the breach to establish injury-in-fact. *Beck*, 848 F.3d at 275; *see also Hutton*, 892 F.3d at 621–22. A plaintiff's plausible allegation of actual misuse of PII—that "their data has been stolen, accessed and used in a fraudulent manner," *Hutton*, 892 F.3d at 622—establishes injury-in-fact since "having one's identity fraudulently misrepresented[ ] is concrete because it either inflicts a tangible injury or will inflict an intangible injury that is on all fours with the common-law tort of appropriation of another's name or likeness," *Holmes*, 156 F.4th at 429 n.18 (internal citations omitted) (citing *Hutton*, 892 F.3d at 622; Restatement (Second) of Torts § 652C). Further, such an allegation of actual misuse may also show that "a substantial risk of harm actually exists" such that "the costs of mitigating measures to safeguard against future identity theft" is no longer too speculative to constitute injury in fact. *See Hutton*, 892 F.3d at 622; *see also Holmes*, 156 F.4th at 434 n.25 ("It may . . . be that mitigation cost is a unique fact such that a plaintiff cannot plead it alone—that mitigation costs must connect with a second injury to be an injury-in-fact." (citing *Hutton*, 892 F.3d at 622)). Finally, where a data breach plaintiff alleges only a publication or dissemination, such an intangible injury must be analogous to a harm actionable at common law to establish standing. *See Holmes*, 156 F.4th at 421–25."); *In*

When it comes to a class representative being the subject of multiple prior data breaches, "[w]here . . . plaintiffs suffer multiple breaches or have their personal information exposed through various unrelated events, they may struggle to prove that any particular injury (including dark-web exposure) is traceable to the breach at issue, undermining standing."[39] "Mere allegations of data exposure or potential misuse are insufficient. Instead, courts have held that plaintiffs must show actual misuse and a connection to the data exposure (traceability) to establish standing."[40] "However, if multiple data breaches at different companies happen simultaneously or close in sequence, plaintiffs with accounts or information profiles at each of these companies may struggle to prove that their harm is traceable to a breach at one particular company."[41] Most courts find traceability to be

re Powerschool Holdings, Inc. & Powerschool Grp., LLC Customer Security Breach Litigation, Case No.: 25-md-03149-BEN-MSB, 2026 WL 772329, at *8 (S.D.Cal. March 18, 2026) ("It is reasonable to infer that postings to the dark web following a data breach are traceable to that breach. *See* Landon v. TSC Acquisition Corp., No. 2:24-cv-03788-SSS-PVC, 2024 WL 5317240, at *4 (C.D. Cal. Nov. 1, 2024). For traceability, a court may consider the cumulative nature of allegations and whether they "fall like dominos, layering on one another to create reasonable inferences" supporting traceability. Bozek v. Arizona Lab. Force, Inc., No. CV-24-02118-PHX-SMB, 2025 WL 264174, at *4 (D. Ariz. Jan. 22, 2025). The following allegations create a reasonable inference that Plaintiffs' injuries are connected to the data breach: (1) they provided their information to PowerSchool; (2) PowerSchool's data was stolen by threat actors; (3) they observed their stolen personal information posted online by the hackers; and (4) they experienced harms related to the data breach. The dark web postings, according to the Complaint, include claims that the information was retrieved from PowerSchool's "PowerSource" portal. Consequently, it is plausible that information exposed in the data breach could have been used and is being used to commit fraud, particularly given the sensitive nature of the PII exposed and its appearance on the dark web. The Court finds that these allegations, combined with the fraudulent transfers that followed, make it at least plausible that the fraudulent transactions Plaintiffs suffered are traceable to the data breach.").

39. *Id.*

40. Matthew M. Morrissey et al., *Courts Reject Theoretical Privacy Violations Due to Lack of Standing*, Faegre Drinker (Apr. 21, 2025), https://www.faegredrinker.com/en/insights/publications/2025/4/courts-reject-theoretical-privacy-violations-due-to-lack-of-standing. Timothy P. Misner, *The Fourth Circuit Used a Data Breach on the Dark Web to Illuminate the Boundaries of Standing*, Robinson Bradshaw Class Actions Brief Blog (Nov. 25, 2025), https://www.classactionsbrief.com/the-fourth-circuit-used-a-data-breach-on-the-dark-web-to-illuminate-the-boundaries-of-standing (elaborating how the Fourth Circuit used a data breach on the dark web as an example of the depths of standing).

41. Lea Schild, Comment, *Ensuring Employee Protection After a Data Breach*, 28 Geo. Mason L. Rev. 1553, 1568–69 (2021) (citing John Biglow, Note, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 Minn. J.L. Sci. & Tech. 943, 961 (2016)).

different than causation or proximate cause, and to be a lesser standard of proof.[42] "[A data subject's] alleged injuries could have resulted from a different data breach, unrelated to [a specific breach], or identity theft unconnected to a data breach at all."[43]

42. Stinson v. Yum! Brands, Inc., No. 3:23-cv-183-DJH-LLK, 2025 WL 2755879, at *8 (W.D. Ky. Aug. 29, 2025), *appeal docketed*, No. 25-5867 (6th Cir. Sept. 26, 2025) ("Finally, Yum contends that [plaintiff] Sidler's injuries are not traceable to Yum's conduct because Sidler does not allege that . . . the same information he provided Yum was used to initiate any alleged unauthorized activity, that he had not been the victim of identity theft before the data breach, or that he has not been previously impacted by a prior data breach. But traceability 'is not focused on whether the defendant caused the plaintiff's injury in the liability sense, . . . because causation to support standing is not synonymous with causation sufficient to support a claim.' Indeed, 'the Supreme Court has made clear that proximate causation is not a requirement of Article III standing.' Instead, the traceability analysis 'mainly serves to eliminate those cases in which a third party and not a party before the court causes the injury.' Ultimately, traceability requires more than speculative but less than but-for causation." (citation modified) (first quoting Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 390 (6th Cir. 2016), and then quoting Lexmark Intern., Inc. v. Static Control Components, Inc., 572 U.S. 118, 134 n.6 (2014)).

43. DiPierro v. Fla. Health Scis. Ctr., Inc., 737 F. Supp. 3d 1314, 1330 (M.D. Fla. 2024) ("Finally, [the plaintiff] suffers from the same hurdle that almost every data breach plaintiff will, even those who can allege misuse: It is far from clear that the three identified instances of fraud are fairly traceable to the Tampa General data breach (or indeed, to any data breach). To be sure, 'traceability does not equate to proximate cause.' Garcia-Bengochea v. Carnival Cruise Corp., 57 F.4th 916, 927 (11th Cir. 2023). But unlike *Garcia-Bengochea*, this is not a situation where the causation inquiry is complicated by multiple actors working in a single chain of events preventing attribution to one alone. *See id.* at 926–27. The question instead is whether the alleged misuse stems from one of many parallel, independent causes, each of which could have resulted in the harm. In *Green-Cooper*, the plaintiffs avoided this problem by alleging that thieves posted the batch of stolen credit cards en masse to a single dark web marketplace, 73 F.4th at 886, thereby rendering traceability quite plausible. Plaintiffs here make no such allegations. And James merely alleges that the data breach occurred prior to the fraudulent credit card charges, which is insufficient without allegations establishing the proximity of the fraudulent charges to the date of the data breach. *See* Am. Compl. ¶ 153. It is possible that the hackers used the information inappropriately themselves. It is also possible that they sold the information directly to another for malfeasance. Or perhaps nothing has happened from the potential exposure of information, at least not based on the episode at Tampa General. That a plaintiff can conjure hypotheticals does not mean that he has plausibly pleaded (much less proven for purposes of final judgment after class certification) traceability."); *see also* Weisenberger v. Ameritas Mut. Holding Co., 597 F. Supp. 3d 1351, 1359 (D. Neb. 2022) ("The defendant's argument suggests that the injuries the plaintiff actually experienced might be the result of an unrelated data breach, but that sug-

Some courts have held definitively that the effect of prior data breaches on the traceability requirement cannot be resolved at the pleadings stage. These courts generally hold that a plaintiff need not plead specific traceability at the pleadings stage,[44] or have held

---

gestion alone does not render causation due to the defendant's data breach implausible. The fairly traceable standard does not equate to a standard of tort causation." (citation omitted)).

44. In *Fero*, the District Court addressed the various approaches:

> In the data breach context, courts have rejected the argument that plaintiffs' injuries are not fairly traceable when their information could have been compromised during a different data breach in recent years. *See Remijas*, 794 F.3d at 696. In *Remijas*, for example, the Seventh Circuit concluded that "[t]he fact that Target or some other store [besides Neiman Marcus] might have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue." *Id.* At the pleading stage, the Seventh Circuit found it sufficient that Neiman Marcus admitted that customers' credit cards had been exposed and that the retailer had notified them that their personal information was at risk. *Id.* The Seventh Circuit explained that Neiman Marcus' argument was better raised as a defense in a later stage in the litigation: "If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then 'the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury.'" *Id.* (citations and quotations omitted).
>
> Other courts have similarly rejected challenges to standing based on traceability in the data breach context, finding the challenge better suited for a later stage of the litigation. See *Lewert*, 819 F.3d at 969 (rejecting the argument that fraudulent charges could not be attributed to data breach at P.F. Chang's, and explaining that the argument that there are potential alternative causes for plaintiffs' injuries may be pursued at merits phase); *In re Zappos.com, Inc.*, 2016 WL 2637810, at *6 (D. Nev. 2016) (rejecting traceability argument because "[w]hether or not . . . [p]laintiffs' allegations suffer from defects that prevent them from ultimately prevailing in the case, the allegations show the connection between the alleged injury and breach is more than just hypothetical or tenuous"); *In re Target Corp.*, 66 F.Supp.3d at 1159 ("Plaintiffs' allegations plausibly allege that they suffered injuries that are 'fairly traceable' to Target's conduct. This is sufficient at this stage to plead standing. Should discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment on the issue.").
>
> On the other hand, in *In re SAIC*, 45 F.Supp.3d at 31–33, the court concluded that some of the plaintiffs did not meet the causation requirement because, while they had alleged unauthorized charges on their credit and debit cards or that money was withdrawn from their bank accounts, none had alleged that credit card, debit card, or bank account information was on the stolen tapes. The district court in *In re: Community Health Systems, Inc.* similarly found that the "fairly traceable" element

that the relevance of other breaches is a question of causation[45] or dam-

exists for purposes of Article III case or controversy standing "when at least one instance of misuse was pled that would have a logical connection to the data stolen." 2016 WL 4732630 at *12. Thus, as in *In re SAIC*, the *In re: Community Health Systems, Inc.* court dismissed, for example, plaintiffs who alleged unauthorized credit card charges but who did not allege that the data breach included credit card information. *See id.* Similarly relying on *In re SAIC*, the D.C. district court in *Welborn* found that a plaintiff who had alleged a potential compromise of her personal information, followed by an instance of fraudulent activity in her financial accounts, such as the removal of funds, could not meet the traceability requirement because "[i]t [wa]s not clear that the type of data obtained from the theft . . . was necessarily used in the removal of funds." 2016 WL 6495399, at *9. That plaintiff thus failed to "put forward facts showing that [her] injuries [could] be traced to the specific data incident of which [she] complain[ed] and not to any previous theft or data loss incident." *Id*. The Court finds Defendants' arguments unpersuasive. The CMC plausibly alleges that the various forms of misuse are "fairly traceable" to the data breach on the Excellus networks. At this early stage of the litigation, Plaintiffs' allegations are sufficient.

Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 757–58 (W.D.N.Y. 2017) (first citing Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015); then citing Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 969 (7th Cir. 2016); then citing *In re* Zappos.com, Inc., No. 2357, 2016 WL 2637810, at *6 (D. Nev. May 6, 2016); then citing *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014); then citing *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 31–33 (D.D.C. 2014); then citing *In re* Cmty. Health Sys., Inc., No. 15-CV-222-KOB, 2016 WL 4732630 (N.D. Ala. Sept. 12, 2016); and then citing Welborn v. Internal Revenue Serv., 218 F. Supp. 3d 64 (D.D.C. 2016)), *on reconsideration*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018), *and order clarified*, 502 F. Supp. 3d 724 (W.D.N.Y. 2020)).

45. *In re* U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 60 (D.C. Cir. 2019) ("That fact, combined with the allegations that at least some of the stolen information was actually misused after the breaches, suffices to support a reasonable inference that Arnold Plaintiffs' risk of future identity theft is traceable to the OPM cyberattacks. Neither the likelihood that some Arnold Plaintiffs experienced other types of unrelated fraud nor the speculative possibility that they might also have been the victims of other data breaches renders causation implausible here."); *see also In re* Zappos.com, Inc., 888 F.3d 1020, 1029 (9th Cir. 2018) ("That hackers might have stolen Plaintiffs' PII in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches . . . , is less about standing and more about the merits of causation and damages."), *cert. denied*, 586 U.S. 1247 (2019); Huynh v. Quora, Inc., No. 18-CV-07597-BLF, 2019 WL 11502875, at *4 (N.D. Cal. Dec. 19, 2019) ("That hackers might have stolen Plaintiffs' PII in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from [Quora]), is less about standing and more about the merits of causation and damages." (quoting *In re*

ages,[46] not of traceability and standing.

One court held that "no court" has accepted the lack-of-standing argument,[47] while others have held that data subjects' victimization by other data breaches has no bearing on standing at the pleadings stage.[48]

Zappos.com, 888 F.3d at 1029)). The Court of Appeals' decision in *Zappos.com* is of questionable validity following the SCOTUS' decision in *Ramirez. I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1054 (N.D. Cal. 2022) ("More fundamentally, in light of *TransUnion*'s rejection of risk of harm as a basis for standing for damages claims, the Court questions the viability of *Krottner* and *Zappos*'s holdings finding standing on this very basis.").

46. *In re* Brinker Data Incident Litig., No. 3:18-cv-686-TJC-MCR, 2021 WL 1405508, at *1 (M.D. Fla. April 14, 2021) *vacated in part*, Green-Cooper v. Brinker Int'l, Inc., 73 F.4th 883, 894 (11th Cir. 2023), *cert. den*, 144 S. Ct. 1457 (2024). *See also DSIR Deeper Dive: Class Certification Jurisprudence*, JD Supra (June 29, 2022) (discussing the district court opinion: "Given the increase in data breaches and the increasing likelihood that a putative class member's information will be subject to multiple breaches, the Brinker court asserted that labeling the multiple-breach issue either a causation or a damages issue "creates a false dichotomy and is not a particularly useful method for deciding predominance." *Id.* Thus, the court found that the multiple-breach issue should be determined at the damages phase. *Id.* With regard to damages, the court found plaintiff's expert to be persuasive. *Id.* The expert asserted that his method of calculating damages included previously breached payment cards because card issuers "work diligently to remove data breach compromised cards from circulation." *Id.* The court acknowledged that a jury might find this methodology is not an accurate reflection of multiple-breach class members' damages but also determined that it is sufficient at this stage of the case. *Id.* The court also noted that if a jury found this methodology inaccurate, there are other methods of calculating damages, such as using an average relative reduction in damages, that may apply. *Id.* Therefore, at this stage of litigation, the court found that damages did not require individualized proof. *Id.*").

47. *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *15–16 (N.D. Cal. May 27, 2016) ("Under Defendants' theory, a company affected by a data breach could simply contest causation by pointing to the fact that data breaches occur all the time, against various private and public entities. This would, in turn, create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable. No California law, the relevant authority addressing causation, or the specific facts of this case support such a legal theory. On the instant motions to dismiss, the Court once again emphasizes: *no* court has ever accepted the Anthem Defendants' argument in the data breach context." (citation modified)).

48. *See* Cohen v. Ne. Radiology, P.C., No. 20-CV-1202, 2021 WL 293123, at *6 (S.D.N.Y. Jan. 28, 2021) (holding although "other data breaches may have exposed his personal information[,]" it "has no bearing on plaintiff's standing to sue"); *Lewert*, 819 F.3d at 969 (stating the defendant's argument regarding potential alternative causes for plaintiffs' injuries may be "pursued at the merits phase").

Still other courts have recognized the issue at the pleadings stage but allowed the case to proceed into the discovery phase.[49] Courts have managed this administratively in a few ways. For example, courts have held that a factual record may be required, after discovery, to determine traceability.[50] Others have surmounted the challenge of F.R.C.P. 12(b)(6) motions being limited to the four corners of the pleadings by relying on "Fact Sheets" submitted by the class representatives as to whether their data was on the dark web.[51] This reflects, by way of analogy, a process similar to the

49. *E.g.*, *In re Mednax Servs., Inc.*, 603 F. Supp. 3d at 1206 ("In support of these arguments, Defendants cite the findings of their experts: Austin Berglas, who led a team of analysts that scoured the dark web to investigate the veracity of these Plaintiffs' allegations, and Kathleen O'Hara, who conducted an exhaustive search of all locations where Mednax would expect Social Security numbers to be located. Because this is a factual challenge, the Court may consider these experts' declarations even though they are presented outside the pleadings. As to the discrepancies in Plaintiffs' PHI and PII between data found on the dark web and that found in Defendants' possession, as discussed *supra* Analysis I.b, even if the data accessed in the Data Breaches did not provide all that was necessary to carry out Plaintiffs' documented incidents of misuse of their information, they conceivably could have been enough to aid therein. And '[e]ven a showing that a plaintiff's injury is indirectly caused by a defendant's actions satisfies the fairly traceable requirement' of standing. As to Defendants' other arguments, without the aid of discovery, the Court is not prepared to find that Plaintiffs' claims warrant dismissal for lack of standing." (citation modified) (quoting Resnick v. AvMed, Inc., 693 F.3d 1317, 1324 (11th Cir. 2012) (quoting Tokyo Gwinnett, LLC v. Gwinnett Cnty., 940 F.3d 1254, 1266 (11th Cir. 2019)).

50. Hood v. Educ. Comput. Sys., Inc., No. 2:24-CV-00666-CCW, 2025 WL 1284737, at *6 (W.D. Pa. May 2, 2025). ("ECSI further asserts that because Plaintiffs appear to concede that they have suffered *multiple* prior instances of identity theft, attributing the misuse of their PII to the Data Breach, as opposed to whatever disclosures enabled prior instances of identity theft, is pure speculation. In response, Plaintiffs argue that they have done enough at this early stage of these proceedings to plausibly allege that their injuries are fairly traceable to the Data Breach. The Court agrees with the Plaintiffs. . . . ECSI's argument that Plaintiffs cannot establish traceability because they suffered multiple prior instances of identity theft, is best decided after discovery and the development of a factual record. *See Gaddy v. Long & Foster Cos., Inc.*, No. CV 21-2396 (RBK)(EAP), 2023 WL 1926654, at *8 (D.N.J. Feb. 10, 2023) ('Although [plaintiff] may not have proof right now that hackers accessed her PII during the Data Breach, it is not her obligation at the pleading stage to prove the allegations.'); *Mielo v. Steak 'n Shake Operations, Inc.*, 897 F.3d 467, 481 (3d Cir. 2018) (finding traceability at the pleading stage where plaintiffs alleged that their injuries were 'caused' by the defendant's unlawful corporate policies)." (citation modified)).

51. *In re* Samsung Data Sec. Breach Litig., 761 F. Supp. 3d 781, 802 (D.N.J. 2025), *appeal docketed*, No. 25-1985 (3d Cir. May 12, 2025) ("And when the Court considers the information contained in the Fact Sheets, it reaches the same result: Plaintiffs fail to establish an injury that is certainly impending or fairly traceable

RICO Worksheet employed by Judge Selna in the Central District of California to weed out unsubstantiated RICO claims at the pleading stage and subjecting RICO complaints to heightened scrutiny at the beginning of litigation.[52]

B. Traceability as a Function of Damages/Risk of Future Harm.

1. *Lost value of PII.*

"A unique element of data breach class actions is that there is generally no single 'metric' of injury to the proposed class, nor a single unifying economic theory of harm."[53] Out-of-pocket expenses, lost time, future costs, and lost value of PII are generic claims of damages that have been rejected by some courts.[54] Using the "market value" for such data raises complications of trying to value such data on either legal or illegal markets.[55]

---

to Defendant. Indeed, the Fact Sheets cast even more doubt as to Plaintiffs' allegations and speculation for several reasons. . . . Second, for three of the four Plaintiffs who alleged that they have been notified that their information is on the Dark Web, the Fact Sheet unequivocally refutes any link to the breach. Plaintiff Baker, who alleged his information is on the Dark Web, stated in his Fact Sheet that Experian notified him that it found 'records associated with [his Social Security Number] on the Dark Web.' As social security numbers were not obtained in this Data Breach, the fact that his data is on the Dark Web is wholly unrelated, and not plausibly traceable, to this breach. Plaintiff Peavy stated in her Fact Sheet that she was first notified that her information was on the Dark Web as early as 2018—four years before the Data Breach in 2022—and as such, this, too, cannot be linked to Defendant. And finally, Plaintiff Allen stated that his email and other 'information' was found on the Dark Web in June 2022—one month before the July 2022 Data Breach." (citations omitted)).

52. Hon. James Selna, *Form Order Regarding RICO Case Statement*, U.S. Dist. Ct. C.D. Cal., https://apps.cacd.uscourts.gov/JpsApi/file/2d3cf60e-eb07-4838-bcb3-223425230399.

53. Branko Jovanovic & Michael Kheyfets, *Value of Personal Information and Data Breach Class Action Settlements*, Edgeworth Econ. (Feb. 20, 2024), https://www.edgeworthеconomics.com/insight-value-personal-info-data-breach-class-action ("Proposed class members might claim harm due to the time spent mitigating potential effects of the breach and the associated loss of productivity, out-of-pocket costs for identity theft protection services, diminution in value of personal information, fraudulent misuse of stolen information, continued risk of future misuse, and loss of the benefit of the bargain with Defendants to provide adequate data security.").

54. *See, e.g.*, Griffey v. Magellan Health Inc., 562 F. Supp. 3d 34, 46–47 (D. Ariz. 2021) (rejecting allegations of "lost time addressing the data breach, continued risk to their PII and PHI, . . . the danger of future harm," "attempted fraud," and the "threat of future injuries" somehow constituted cognizable injuries).

55. Given this set of economic characteristics, it is unlikely that generic statistics from public sources purporting to represent "market value" can serve as reliable proxies of the "lost value of information" for any individual class member in a data breach litigation. However, economic arguments and techniques are

Accordingly, "courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value,"[56] although, again, some courts find that deciding that issue cannot be done at the pleadings stage.[57]

---

likely to continue evolving as data privacy litigation analysis continues to mature.

Michael Kheyfets, *Litigation, Professional Perspective—Value of Personal Information Theories in Data Privacy Class Actions*, Bloomberg L. (Sept. 2022), https://www.bloomberglaw.com/external/document/X1LHTVQS000000/litigation-professional-perspective-value-of-personal-information.

56. Wilkins v. Eng. Const. Co., Inc., No. 6:24-CV-00059, 2026 WL 657758, at *3 (W.D. Va. Mar. 9, 2026) (quoting Podroykin v. Am. Armed Forces Mut. Aid Ass'n, 634 F. Supp. 3d 265, 272 (E.D. Va. 2022) ("Regarding the fourth harm set forth in the Amended Complaint—i.e., diminution in value of their PII—Plaintiffs have not alleged that they could or would sell their Social Security numbers, drivers' license numbers, dates of birth, or addresses, for money. Moreover, much of that information is only valuable to criminals. Presumably, Plaintiffs would not sell their own Social Security numbers to cybercriminals who, in turn, would use that information to cause Plaintiffs' financial harm. Therefore, it is entirely unclear how Plaintiffs' Social Security and driver's license numbers have legitimate monetary value that could be diminished by public disclosure. Because Plaintiffs have not alleged that they would have or could have sold the PII that was stolen from English's computers, their diminution in value argument has no legs." (citations omitted)); *accord* Welborn v. IRS, 218 F. Supp. 3d 64, 78 (D.C. 2016) (collecting cases); *see also* Willingham v. Glob. Payments, Inc., No. 1:12-CV-01157-RWS, 2013 WL 440702, at *7 (N.D. Ga. Feb. 5, 2013) ("Plaintiffs' PII does not have an inherent monetary value."); *In re* Arthur J. Gallagher Data Breach Litig., 631 F. Supp. 3d 573, 592 (N.D. Ill. 2022) (explaining how courts in the data breach context have "routinely rejected the proposition that an individual's personal identifying information has an independent monetary value.") (internal quotation marks omitted) (quoting *Fero* v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 755 (W.D.N.Y. 2017); Irwin v. Jimmy John's Franchise, LLC, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016) (dismissing unjust enrichment claim because the plaintiff "did not pay for a side order of data security and protection; it was merely incident to her food purchase, as is the ability to sit at a table to eat her food, or to use Jimmy John's restroom"); *see also* Perdue v. Hy-Vee, Inc., 455 F. Supp. 3d 749, 766 (C.D. Ill. 2020) (dismissing unjust enrichment claim); Gordon v. Chipotle Mexican Grill, Inc., 344 F. Supp. 3d 1231, 1249 (D. Colo. 2018) ("Plaintiffs paid for burritos; Plaintiffs received burritos."). *See generally* Comment, *What is My Self-Worth: An Analysis of California's Statutory Protections for Personal Information*, 16 Wake Forest L. Rev. Online 28 (2026).

57. *In re* New Era Enters. Inc. Data Incident Litig., No. CV H-25-732, 2026 WL 303547, at *9 (S.D. Tex. Feb. 4, 2026) ("The complaint alleges that personally identifiable information has market value, which the data breach diminished by making the information readily accessible on the dark web. New Era cites cases finding similar allegations insufficient because the plaintiffs did not allege

2. *Actual and future harm.*

"[A]ctual damages are necessary to the cause of action."[58] Although, generally, courts have held that "an increased risk of future harm alone is insufficient to show damages,"[59] data subjects still turn to the risk of future harm to support standing. First, data breaches seldom result in identity theft, anyway.[60]

The Court of Appeals for the Second Circuit adopted a three-part analysis for whether threat of future harm is sufficient for Article III standing in *McMorris v. Carlos Lopez & Associates, LLC*[61]: (1) whether the plaintiff's data has been exposed as the result of a targeted attempt to obtain that data, such as a hacking incident or data breach by a malicious third party; (2) whether any portion of the data acquired had already been misused, even if the plaintiffs themselves had not yet been the subjects of identity theft or fraud; and (3) whether the type of data that has been exposed is of such a sensitive nature that the risk of identity theft or fraud is heightened.[62]

---

that they will attempt to sell, or have in the past sold, their personally identifiable information. This logic is unpersuasive because in other contexts plaintiffs may recover the lost value of their damaged property without showing that they plan to sell it. . . . These principles apply to the allegations by some of the plaintiffs that New Era's negligence caused their personal information to be posted on the dark web, and diminished the market value of their property (their personally identifiable information). New Era's argument may prove persuasive at the summary-judgment stage or at trial, when the plaintiffs must produce evidence that their personally identifiable information has lost value. A factfinder might not find that the plaintiffs have been harmed because they cannot show that they would sell their data soon or that they can only do so at a diminished price. But at this stage in the litigation, the court must take the plaintiffs' allegations as true. The plaintiffs have sufficiently alleged a diminution in the market value of their personally identifiable information." (citations omitted)).

58. *In re* Trans Union Corp. Priv. Litig., 211 F.R.D. 328, 346 (N.D. Ill. 2002) (quoting Restatement (Second) Torts § 907 cmt. a (Am. L. Inst. 1965)); *see also* Dominion Nutrition, Inc. v. Cesca, 467 F. Supp. 2d 870, 884 (N.D. Ill. 2006) ("Nominal damages are not awarded for negligence.").

59. McGlenn v. Driveline Retail Merch., Inc., No. 18-CV-2097, 2021 WL 4301476, at *9 (C.D. Ill. Sept. 21, 2021) (explaining a present injury is required).

60. U.S. Gov't Accountability Off., GAO-07-737, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown 30 (2007) [hereinafter GAO REPORT], https://www.gao.gov/new.items/d07737.pdf [https://perma.cc/85RM-VB9U] (explaining personal information can be used to open new accounts or incur actual financial charges).

61. McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295 (2d Cir. 2021).

62. *Id.* at 303.

But data subjects' victimization in multiple unrelated data breaches may defeat their claims of proving actual or future harm.[63] In other words, the subjects' history of breach may negate the second prong of the *McMorris* test. Multiple data breaches matter to determine "what" data was the subject of each breach.[64] Allegations that different data from different breaches could form a matrix from which identity thieves could create an identity profile, however, could survive a motion to dismiss.[65] Some courts

63. Polkowski v. Jack Doheny Cos., Inc., No. 2:25-CV-10516, 2025 WL 3079358, at *7 (E.D. Mich. Nov. 4, 2025) ("First, JDC offers evidence that the phishing emails purporting to be about car insurance, which Plaintiff complained of, cannot be attributed to the Data Breach because the Plaintiff's Gmail account was disclosed in at least five previous and unrelated data breaches dating back as far as 2018 and as recently as 2024. Next, JDC provides evidence that Plaintiff cannot show that any alleged mitigation costs were reasonably incurred, as required by *Galaria*, because he declined the free credit monitoring services; and moreover, there is no mention in the Complaint that Plaintiff actually incurred out of pocket mitigation costs, making it distinguishable from the injuries deemed cognizable in *Galaria* and *In re Flagstar*. The Court agrees on both points and finds Defendant's traceability argument persuasive with respect to the actual *and* future harms alleged by the Plaintiff." (citation modified)).

64. Cantinieri v. Verisk Analytics, Inc., No. 21-CV-06911 (JMA) (JMW), 2023 WL 2734682, at *2 (E.D.N.Y. Mar. 31, 2023) ("Second, and perhaps more importantly, if the data breach did not result in disclosure of sensitive data elements—such as Social Security numbers—that could have caused Plaintiff's alleged injuries-in-fact, those harms would not be 'fairly traceable to' the data breach. *Cooper v. Bonobos, Inc*., No. 21-CV-854, 2022 WL 170622, at *2–4 (S.D.N.Y. Jan. 19, 2022) (citation omitted); *see also, e.g*., *In re* Uber Techs., Inc., Data Sec. Breach Litig., No. 18-CV-182970, 2019 WL 6522843, at *6 (C.D. Cal. Aug. 19, 2019) (plaintiff's alleged injuries were not 'fairly traceable' to data breach because it was not apparent 'how the disclosure of Plaintiff's basic contact information and driver's license number could be plausibly used to gain access to his tax return or make fraudulent charges on his credit and debit cards'). The Court finds the reasoning of *Cooper* and *In re Uber* persuasive. Thus, the Court agrees with Defendants that—at the very least—the critical question here is whether Plaintiff's Social Security number (or other sensitive data that could have caused Plaintiff's alleged injuries-in-fact) was obtained or exposed in the data breach."). *But see* Maser v. Commonspirit Health, No. 1:23-cv-01073-RM-SBP, 2024 WL 2863579, at *7 (D. Colo. Apr. 16, 2024) (finding consumer could not link bank fraud to data breach where bank information was not exposed); Almon v. Conduent Bus. Servs., LLC, No. SA-19-CV-01075-XR, 2022 WL 902992, at *22–23 (W.D. Tex. Mar. 25, 2022) (granting summary judgment where "discovery has not provided any evidence tying unauthorized activity on their accounts to a data breach involving Defendants").

65. Olson v. Ferrara Candy Co., 275 N.E. 3d 439, 454 (Ill. App. 2025), *appeal denied*, No. 132021, 2025 WL 3302000 (Ill. App. Nov. 26, 2025) ("Regarding traceability, Ferrara argues that the alleged harm of the unauthorized charges to [Plaintiff] Wesson's credit union account is not fairly traceable to the data breach because, as stated in the declaration from Ferrara's director of cyber-

refer to this as the "mosaic effect."[66] The "mosaic effect" argument, however, has not been well received because it turns on speculation of the actions of a third party, and a criminal actor at that–namely, the malicious actors or the purchasers of data on the dark web–in violation of the "fairly traceable" standard of causation.[67]

---

security, Ferrara never had any information concerning Wesson's credit union account. We disagree. Drawing all reasonable inferences from the operative complaint at the motion to dismiss stage, we conclude that plaintiffs allege a sufficient connection between the actual misuse of Wesson's PII and the data breach. Wesson alleged that two short months after the data breach, he was the victim of attempted fraudulent charges to his credit union account. Moreover, he was not aware of any other data breaches or reasons why criminals would have his credit union account information other than because of Ferrara's data breach that exposed certain of his PII. Plaintiffs also alleged that, as a result of Ferrara's data breach, cybercriminals were now able to cross reference multiple sources of plaintiffs' PII to compile Fullz packages that can be used for further identity theft and fraud, as experienced by Wesson."); *In re* Unite Here Data Sec. Incident Litig., 740 F. Supp. 3d 364, 376 (S.D.N.Y. 2024) ("Defendant argues that plaintiffs have failed to satisfy the traceability element because 'there is a good chance that one or both Plaintiffs has already had her personal information exposed' in any one of the many major data breaches that have occurred in the U.S. recently. UNITE MTD, at 11. This argument ignores the procedural posture of the case. . . . As explained above, the complaint plausibly alleges that plaintiffs were subject to an increased risk of identity theft because important and sensitive information was stolen in the breach. Further, the complaint describes in some detail how compounding data breaches can increase the risk of identity theft as stolen information is compiled from multiple sources and used by criminals. *See* Compl. ¶¶ 70–89; *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 31-32 (D.D.C. May 9, 2014) (giving plaintiffs 'the benefit of the doubt' on traceability even if '[n]o one alleges that credit-card, debit-card, or bank-account information was' breached). Therefore, the complaint easily satisfies the traceability requirement."), *motion to certify appeal denied*, No. 24-CV-1565 (JSR), 2024 WL 4307975 (S.D.N.Y. Sept. 26, 2024).).

66. Salas v. Acuity-CHS, LLC, No. 22-317-RGA, 2023 WL 2710180, at *6 (D. Del. Mar. 30, 2023) ("Ms. Salas points to the 'mosaic effect,' by which cybercriminals piece together multiple data sources to reveal new private information about individual.").

67. Standing requires a "causal connection" between the injury and the conduct complained of—the injury must be "fairly traceable" to the defendant and not the result of "independent action of some third party not before the court." *Lujan*, 504 U.S. st 560 (citation modified). Plaintiffs' alleged future injuries hinge on speculation about the "independent actions" of third-party cybercriminals not before the Court, which is insufficient to trace plaintiffs' alleged injuries to defendants' conduct. *See, e.g.*, Engl v. Nat. Grocers by Vitamin Cottage, Inc., No. 15-cv-02129-MSK-NYW, 2016 WL 8578096, at *7 (D. Colo. June 20, 2016), *report and recommendation adopted*, No. 15-CV-02129-MSK-NYW, 2016 WL 8578252 (D. Colo. Sept. 21, 2016) ("The proposition that the hackers who carried

Thus, courts have also mixed elements of traceability with elements of causation under a standing analysis to conclude that causation is difficult to prove where the data subject was the victim of multiple breaches.[68] Courts also have analyzed mere "posting" on the dark web versus actual use of the data subjects' data "from" the dark web.[69] Although it is true

---

out the Cyberattack are using [the] information gained in the attack in connection with other information identified on the Internet or from other cybercriminals or that the hackers intend to do so in the future, which is conditioned solely on the actions of unknown third parties is simply too attenuated."); McCombs v. Delta Grp. Elecs., Inc., 676 F. Supp. 3d 1064, 1073 (D.N.M. 2023) ("The Court is reluctant to infer a causal connection between the alleged bank account access and the data breach almost a year prior when [plaintiff] fails to sufficiently substantiate her claim.").

68. Castillo v. Seagate Tech., LLC, No. 16-cv-01958-RS, 2016 WL 9280242, at *4 (N.D. Cal. Sept. 14, 2016) ("To state a claim for negligence, plaintiffs must plead facts that plausibly connect the alleged breach of duty to the harm plaintiffs suffered. *In re* Sony, 996 F. Supp. 2d at 964. After learning about the phishing attack, each named plaintiff discovered that tax returns had been filed using his or her personal identifying information. This raises a reasonable inference the person who filed the fraudulent tax return obtained plaintiffs' personal identifying information from the Seagate phisher—information obtained allegedly due to Seagate's lax security measures. Tran's case, however, is different. She concedes her personal identifying information had been compromised during a previous, unrelated data breach. Compl. ¶ 28. She has thus not provided sufficient information to conclude her 2015 federal tax return was filed as a result of the Seagate data breach. An equally strong inference, on the basis of these facts, is that the fraudulent 2015 tax return was traceable to the fact that her personal information already circulated among certain cyber scoundrels. To create a reasonable inference the Seagate data breach caused the 2015 filing, Tran should plead more particular facts connecting the two events, such as the temporal relationship between the breach and the false filing, or the similarities between the false filing in her name and the filings in the names of other Seagate personnel.") (citing *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 964 (S.D. Cal. 2012)).

69. Prestby v. A&A Servs., LLC, No. 8:24CV204, 2026 WL 26128, at *9 (D. Neb. Jan. 5, 2026) ("[Plaintiffs] Moser and Sutherlin claim they experienced actual misuse because their Private Information is now posted on the dark web and has likely been sold or is available for sale to a cybercriminal. However, in *Super[V]alu*, the plaintiffs alleged their credit card information was harvested by cybertheft, the defendants' lax security practices made that theft possible, plaintiffs' credit card information was stolen, and 'on information and belief,' illicit websites were selling their credit-card information to counterfeiters and fraudsters. *SuperValu* disregarded the allegation made 'on information and belief' as speculative and held that the plaintiffs' remaining allegations were sufficient to show credit-card theft but not actual harm from misuse of the stolen information. Likewise, the allegation that the plaintiffs' identifying information was posted on the dark web supports a finding of theft, but absent some nonspeculative allegation that the information has been used without authorization

that some courts have employed a burden-shifting analysis in such a data breach scenario.[70]

C. Traceability to Defeat Class Certification.

1. *Improper class representative.*

It is axiomatic that, as addressed above, if the class representative lacks standing, then the class representative cannot represent the class. If the class representative can establish standing, however, the inquiry does not end there.

First, multiple prior data breaches can raise serious questions about the representative's trustworthiness, diligence, and ability to protect class members' interests. If the representative has a history of mishandling sensitive information, it may suggest a conflict of interest or a failure to meet the fiduciary duty owed to absent class members.

Moreover, the claims and defenses of the class representative must be typical of the claims and defenses of the class.[71] The typicality requirement is intended to preclude certification of those cases where the legal theories of the named plaintiff potentially conflict with those of the absent class members.[72]

---

by a third party, Moser and Sutherlin have failed to allege an actual misuse of their Private Information traceable to the Sav-Rx data breach.") (citation omitted) (quoting *In re* SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017)).

70. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015) ("If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then 'the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the "but-for" cause of the plaintiff's injury.'") (quoting Price Waterhouse v. Hopkins, 490 U.S. 228, 263 (1989) (O'Connor, J., concurring); Portier v. NEO Tech. Sols., No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *10 (D. Mass. Dec. 31, 2019) ("The fact that Plaintiffs' PII might have been exposed through an unrelated data breach does nothing to negate the plaintiffs' standing to sue. It is certainly plausible for pleading purposes that their injuries are 'fairly traceable' to the data breach at [NEO Tech]. If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." (citation modified) (quoting *Remijas*, 794 F.3d at 696)), *report and recommendation adopted*, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *In re* Snowflake, Inc., No. 2:24-MD-03126-BMM, 2025 WL 3023009, at *5 (D. Mont. Oct. 29, 2025) ("Defendants do not rely explicitly on other data breaches, but instead emphasize that credit card fraud occurs every day, and that there are countless other reasons why a fraudulent transaction might occur. Defendants attempt to make the same argument rejected by the court in *In re Equifax* [and] *Remijas*. . . .") (internal quotation marks omitted and citations).

71. Fed R. Civ. P. 23(a)(3).

72. Gen. Tel. Co. of Sw. v. Falcon, 457 U.S. 147, 156 (1982); Orr v. Shicker, 953 F.3d 490, 500 (7th Cir. 2020).

Thus, typicality is lacking when the purported class representative is subject to unique defenses that could not be asserted against the class.[73] A named plaintiff is neither typical nor adequate if "there is a danger that absent class members will suffer if their representative is preoccupied with defenses unique to it."[74] A class representative who was subject to multiple prior data breaches that affected standing, causation, and damages might be preoccupied with defending such defenses, such that the class representative would not be a proper representative.

2. *Manageability/typicality/superiority.*

The corollary to a class representative preoccupied with defending their own defenses, which are unique from the class, is whether putative class members share similar preoccupation problems with their own claims. Where "the main issues in a case require the separate adjudication of each class member's individual claim or defense, a Rule 23(b)(3) action [is] inappropriate."[75] Individual questions require each class member "to present evidence that varies from member to member," while common questions can be answered by "the same evidence . . . for each member . . . [or] the issue is susceptible to generalized, class-wide proof."[76] When a defendant "invoke[s] an individualized issue . . . and provide[s] evidence that at least some class members lack meritorious claims because of this issue," the

73. Ellis v. Costco Wholesale Corp., 657 F.3d 970, 984 (9th Cir. 2011) (explaining class representative does not meet typicality requirements if representative will be preoccupied with defenses unique to representative); DZ Reserve v. Meta Platforms, Inc., 96 F.4th 1223, 1238 (9th Cir. 2024) (noting a named plaintiff is neither typical nor adequate if "there is a danger that absent class members will suffer if their representative is preoccupied with defenses unique to it"); Lineberry v. AddShoppers, Inc., No. 23-cv-01996-VC, 2025 WL 1533136, at *2 (N.D. Cal. May 29, 2025) ("[T]o put it more directly, a named plaintiff is not typical or adequate if the jury could realistically rule against them on a basis that wouldn't apply to the rest of the class.").

74. DZ Reserve, 96 F.4th at 1238 (citation omitted); *see also* Brinkley v. Monterey Fin. Servs., LLC, No. 16-CV-01103-RSH-WVG, 2022 WL 4111871, at *5 (S.D. Cal. Sept. 8, 2022) (demonstrating whether plaintiff impliedly consented to recordings would be a "major focus of the litigation"). "Or, to put it more directly, a named plaintiff is not typical or adequate if the jury could realistically rule against them on a basis that wouldn't apply to the rest of the class." *Lineberry*, 2025 WL 1533136, at *2 (citation omitted). Nor is a plaintiff adequate if they have a "conflict[] of interest" with "the class they seek to represent." Woods v. Google LLC, No. 11-cv-01263-EJD, 2018 WL 4030570, at *4 (N.D. Cal. Aug. 23, 2018) (citation omitted). The adequacy requirement is "key to the integrity of class action litigation" and "perhaps the most significant of the prerequisites to a determination of class certification." *Id.* (citation omitted).

75. Zinser v. Accufix Rsch. Ins., Inc., 253 F.3d 1180, 1189 (9th Cir. 2001).

76. Tyson Foods, Inc. v. Bouaphakeo, 577 U.S. 442, 453 (2016) (internal quotation marks and citation omitted).

"spectre of class-member-by-class-member adjudication" is raised.[77] "Where resolving claims would require conducting many inquiries on an individual basis, neither of the predominance or superiority requirements are met."[78]

The presence of vastly different types of data and experiences will require the court to review each individual class member's compromised data and individual circumstances to ensure proper adjudication of each person's claims and alleged injuries. Moreover, as demonstrated by dark web research, a significant number of class members will likely have been subject to prior data breaches, which will distinguish and further complicate their cases from those who were not victims of prior data breaches. Courts have denied certification where the following individualized questions predominated: (1) whether each class member actually experienced identity theft; (2) whether the identity theft was traceable; (3) whether the class member previously took measures to protect their personal information from theft; (4) when and whether each class member enrolled in the credit and identity monitoring offered by defendant; and (5) whether each class member relied on defendant's representations regarding the breach and the procedures in place to safeguard personal information.[79] Similarly, "[i]ndividualized issues on causation, injury, and damages will require more than the common questions."[80] An attempt to narrow class members to those whose data was not the subject of prior data breaches raises identification problems, as the inability to identify customers defeats superiority.[81]

---

77. *See* Van v. LLR, Inc., 61 F.4th 1053, 1069 (9th Cir. 2023).

78. Mobile Emergency Hous. Corp. v. HP, Inc., No. 20-cv-09157-SVK, 2023 WL 9550942, at *12 (N.D. Cal. Dec. 8, 2023).

79. Gardner v. Health Net, Inc., No. CV 10-2140 PA (CWx), 2010 WL 11579028, at *4 (C.D. Cal. Sept. 13, 2010); *see also* S. Indep. Bank v. Fred's, Inc., No. 2:15-CV-799-WKW, 2019 WL 1179396, at *20 (M.D. Ala. Mar. 13, 2019) (denying certification where individualized damages worked against predominance and there was evidence that fraud was caused by something other than breach at issue).

80. McGlenn v. Driveline Retail Merch., Inc., No. 18-cv-2097, 2021 WL 165121, at *6 (C.D. Ill. Jan. 19, 2021). In *McGlenn*, the court denied class certification in a data breach relating to an email phishing scam where a "detailed analysis of proximate cause" was necessary for each class member. *Id.* at *9. As described here, several members of the class had been involved in other data breaches, and the defendant "ha[d] raised doubt as to whether Plaintiff and other class members have actually suffered any injury." *Id.* at *10. Accordingly, the commonality and predominance requirements were not met and the court denied class certification. *Id.* at *5, *10.

81. Walker v. Life Ins. Co. of the SW., 953 F.3d 624, 632–33 (9th Cir. 2020) (courts may consider difficulties identifying class members under predominance or superiority requirement); Briseno v. ConAgra Foods, Inc., 844 F.3d 1121, 1126

Finally, and relatedly, multiple-compromised data or data subjects raise questions about whether individual class-member standing questions predominate. The United States Supreme Court has held that each putative class member must have standing.[82] Manageability problems predominate where a court is called on to determine whether each class member who previously had been the victim of unrelated data breaches had standing.

3. *Multiple-compromised data and data subjects raise questions of certifiability of an injunctive relief class.*

"Rule 23(b)(2) allows class treatment when 'the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.'"[83] Thus, "[t]he key to the (b)(2) class is the indivisible nature of the injunctive or declaratory remedy warranted—the notion that the conduct is such that it can be enjoined or declared unlawful only as to all of the class members or as to none of them."[84] And, an injunction cannot be based on speculative conduct regarding the future handling of data by a malicious actor.[85]

(9th Cir. 2017) (superiority mandates considering "likely difficulties in managing a class action").

82. Each class member must have Art. III standing. Ramirez, 594 U.S. at 431 (explaining in a Rule 23 class action, "[e]very class member must have Article III standing in order to recover individual damages," because "Article III does not give federal courts the power to order relief to any uninjured plaintiff, class action or not" (quoting Tyson Foods, Inc. v. Bouaphakeo, 577 U.S. 442, 466 (2016) (Roberts, C.J., concurring))); Elzen v. Advisors Ignite USA LLC, No. 22-C-859, 2024 WL 195473, at *5 (E.D. Wis. Jan. 18, 2024) (quoting Ramirez, 594 U.S. at 431); Vargo v. Casey, 756 F. Supp. 3d 672, 680 (W.D. Wis. 2024) ("The Judiciary's role is limited 'to provid[ing] relief to claimants, in individual or class actions, who have suffered, or will imminently suffer, actual harm.'" (quoting *Tyson Foods*, 577 U.S. at 466)); *In re* Blackbaud, Inc., No. 3:20-mn-02972-JMC, 2021 WL 1313552, at *2 (D.S.C. Apr. 8, 2021) ("Thus, disclosure of the identities of Defendant's customers will allow Class Counsel to determine whether putative class representatives received data breach notification letters from one of Defendant's customers. If putative class representatives received letters from organizations unrelated to Defendant and their personal information was disclosed as a result of a different data breach, they will be unable to establish the causation element of standing for this case and would not be appropriate putative class representatives.").

83. Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 360 (2011) (emphasis added).

84. *Id.* (citation omitted).

85. Holmes v. Elephant Ins. Co., 156 F.4th 413, 431–32 (4th Cir. 2025) ("All this means that fraudulent impersonation will befall Cardenas and Holmes only if *other* intervening malicious actors acquire their driver's license numbers from the dark web *and* also acquire other pieces of their personal information *and* do so before their driver's license numbers change. And under our precedent, the plaintiffs cannot just assert that all this *might* happen; they must allege facts

The risk of identity theft for multiple-compromised data subjects is unprovable. For prior conduct, the data subject must show "either continuing, present adverse effects due to [his] exposure" to the data holder or "a sufficient likelihood that [he] will again be wronged in a similar way."[86] Rule 23(b)(2) certification "applies only when a single injunction or declaratory judgment would provide relief to each member of the class" and "does not authorize class certification when each individual class member would be entitled to a *different* injunction or declaratory judgment against the defendant" nor "when each class member would be entitled to an individualized award of monetary damages."[87] A Rule 23(b)(2) injunctive relief class requires both risk of irreparable injury and commonality of the single injunction that will address the risk for each putative class member.

This is where prior data breaches make a request for injunctive relief stumble: A multiple-compromised data subject will remain subject to virtually the same pre-existing identity theft risk both before and after the data breach at issue. An injunction will not eliminate the risk, as reflected by the fact that a multiple-compromised data subject could be the subject of multiple injunctions arising from prior class action settlements—none of which prevented the data breach in a particular case. Individual assessments of each class member's data history would be required to determine whether the member is entitled to injunctive relief.[88] Each class member still would need Article III standing to pursue injunctive relief.[89] A data breach class member must demonstrate a "threat of injury [that is] 'actual and imminent, not conjectural or hypothetical.'"[90]

---

allowing us to conclude that for some particular plaintiff, the combined probability of that speculative chain materializing surpasses at least 33%.").

86. Campbell v. Facebook, Inc., 951 F. 3d 1106, 1119–20 (9th Cir. 2020) (internal quotation marks and citations omitted).

87. Jennifer Dickey, *Lessons from Equity for Rule 23(b)(2) Class Actions*, U.S. Chamber of Comm. (December 14, 2022), https://www.uschamber.com/lawsuits/lessons-from-equity-for-rule-23b2-class-actions (quoting Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 360 (2011)).

88. *See, e.g.*, Ginwright v. Exeter Fin. Corp., 280 F. Supp. 3d 674, 690 (D. Md. 2017) (denying certification of TCPA injunction class where "the legality of autodialed calls to individual class members depends on whether the class member consented to receive calls and never revoked that consent"); Ung v. Universal Acceptance Corp., 319 F.R.D 537, 544 (D. Minn. 2017) (same). As in *Ginwright*, "[b]ecause appropriate injunctive relief would require individual assessments of whether the particular class members are entitled to an order barring additional calls to them, certification under Rule 23(b)(2) is not warranted." *Ginwright*, 280 F. Supp. 3d at 690.

89. *See* Hodgers-Durgin v. de la Vina, 199 F.3d 1037, 1045 (9th Cir. 1999) (explaining Article III standing separately is required to seek the requested injunctions).

90. Davidson v. Kimberly-Clark Corp., 889 F.3d 956, 967 (9th Cir. 2018) (citation omitted).

V. Conclusion

As data breaches escalate in frequency and scale, the reality that most data subjects' information has been compromised multiple times is reshaping the landscape of class action litigation. The dark web—a sprawling, anonymous marketplace where stolen data is bundled, priced, and resold—serves a key role in both propelling breaches and serving as a source of evidence in defending class actions. For defendants, dark web investigations and expert forensic testimony offer powerful tools to challenge Article III standing, class certification, and availability of injunctive relief by demonstrating that a plaintiff's data was already available on the dark web from prior, unrelated breaches, thereby undermining the traceability of any alleged injury to the breach at issue.

Courts remain divided on when and how traceability should be evaluated, with some resolving the question at the pleading stage, others deferring to discovery, and still others employing creative procedural mechanisms such as plaintiff fact sheets. These same issues must be tackled in the class certification analysis. Multiple-compromised data subjects raise significant challenges to typicality, predominance, superiority, and the viability of injunctive relief classes. Defense counsel would be well served to invest early in dark web forensic analysis and expert engagement. A data-centric and data subject-centric defense strategy will be indispensable in the years ahead.